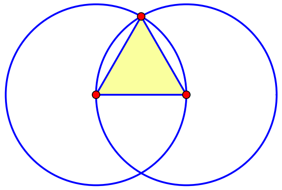
Quod Erat Demonstrandum

—

Inzien en Bewijzen



Jan van Eijck en Albert Visser

8 september 2004

Inhoudsopgave

Hoofdstuk 1

Het Hart van de Exacte Wetenschap

1.1 Het belang van bewijzen

Als je de stof in de wiskunde boeken die je tot nu toe in handen hebt gehad niet interessant vindt zou dat een teken kunnen zijn van zeer goede smaak. In die boeken wordt namelijk stelselmatig verdonkeremaand waar het bij wetenschappelijk denken echt om gaat. Het hart van de exacte wetenschappen wordt gevormd door het begrip *bewijs*. De ontdekking van de methode om een onderwerp te presenteren in termen van axioma's, definities en bewijzen is één van de grote uitvindingen van de Mensheid. Het beroemdste voorbeeld van deze axiomatische methode is de systematische presentatie van meetkundige inzichten in de *Elementen* van Euclides, geschreven tussen 330 en 320 voor Christus. Om toegang te krijgen tot cultuurschatten zoals deze moet je vertrouwd raken met de gebruikte manier van presenteren.

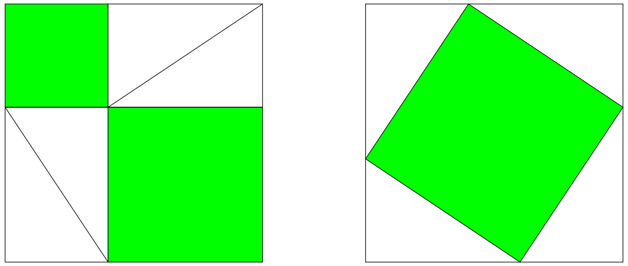
Het stramien van een bewijs in Euclides' *Elementen* is heel strak. Alle bewijzen beginnen met een opsomming van wat gegeven is, gevolgd door "te bewijzen:", met daarna de bewering waarvan de waarheid moet worden aangetoond. Dan volgen de stappen die nodig zijn om de "te bewijzen" bewering af te leiden uit wat gegeven is. Door de stappen te volgen kun je inzien dat de "te bewijzen" bewering waar moet zijn. In die bewijsstappen kunnen ook beweringen worden gebruikt die al eerder bewezen zijn. Zulke al bewezen beweringen heten *stellingen*. Het bewijs eindigt wanneer we zijn aangeland bij de bewering die bewezen moet worden. De laatste zin van het bewijs luidt: 'en dat is precies wat moest worden aangetoond'. De latijnse versie van deze afsluitende frase is *quod erat demonstrandum*, afgekort *QED* (in het Grieks stond er: $o\pi\epsilon\rho\ \epsilon\delta\epsilon\iota\ \delta\epsilon\tilde{\iota}\xi\alpha\iota$). Dit is nog steeds een veelgebruikte afkorting om aan te geven dat een bewijs rond is. En als een bewijs rond is, is er een nieuwe stelling toegevoegd aan de lijst van stellingen. Zo groeit onze kennis stapje voor stapje.

Eén van de stellingen die in het eerste boek van Euclides' *Elementen* worden bewezen is de stelling van Pythagoras:

> In een rechthoekige driehoek is de som van de kwadraten van de rechthoekszijden gelijk aan het kwadraat van de schuine zijde.

Een bewijs van een stelling heb je wanneer je kunt laten zien dat die stelling waar is. Zie

opdracht 1.1.



Figuur 1.1: Een bewijs van de stelling van Pythagoras in de vorm van twee plaatjes.

Opdracht 1.1 *Leg uit waarom de twee plaatjes in Figuur 1.1 een bewijs vormen van de stelling van Pythagoras. Een bewijs van een stelling heb je wanneer je kunt laten zien waarom die stelling waar is. Hoe laten de twee plaatjes zien dat de stelling van Pythagoras waar is? (Dit plaatjesbewijs is overigens niet het bewijs dat Euclides geeft.)*

Wiskundige bewijzen leren begrijpen en zelf opzetten vormde eeuwenlang de hoofdmoot van het wiskunde-onderwijs. Vandaag de dag is dat niet meer zo, omdat 'inzicht verwerven' belangrijker wordt geacht dan vaardigheid krijgen in het bewijzen. Bewijs en inzicht zijn echter twee kanten van dezelfde medaille: door te proberen bewijzen te leveren of doorgronden kom je tot inzicht, en om inzicht te communiceren zijn bewijzen nodig.

Dit boek maakt duidelijk hoe centraal het begrip 'bewijs' is in de ontwikkeling van het exacte denken. Je gaat in dit boek leren hoe je zelf bewijsproblemen kunt aanpakken. Dan zul je ontdekken dat zelf leren bewijzen een uitstekende manier is om toegang te krijgen tot de wereld van de exacte wetenschap. Dat toegangsrecht krijg je niet cadeau: je moet het verdienen. Zelf bewijzen leren leveren is moeilijk, en wat moeilijk is, is alleen weggelegd voor wie talent heeft en bereid is zich in te zetten. Maar wie het wil leren zou daarbij geholpen moeten worden. In dit boek maken we daarmee een begin.

Het feit dat leren bewijzen nu is voorbehouden aan de echte 'liefhebbers' heeft in elk geval als voordeel dat er zo niemand die daar geen zin in heeft met echte wiskunde wordt geplaagd. Of wiskundig denken iets voor jou is kun je in de bladzijden die volgen zelf gaan ontdekken. Wij geven in de rest van dit hoofdstuk een paar voorbeelden van prachtige bewijzen uit de Klassieke Oudheid. Als je die bewijzen leuk vindt is er kans dat er met dit boek een nieuwe wereld voor je open gaat. Vind je er niets aan, dan is dat ook nuttige informatie. Gevaar dat je verloren gaat voor de wetenschap is er dan hoegenaamd niet: dit pad van het denken en weten is dan kennelijk niet jouw weg.

Wat wiskunde te bieden heeft is inzicht met eeuwigheidswaarde. Het inzicht dat de wortel uit twee geen breuk is is een inzicht voor alle tijden. Het feit dat mensen zulke inzichten kunnen verwerven is een van de grote wonderen van het bestaan. Het besef dat het mogelijk is sommige dingen volstrekt klaar en duidelijk in te zien zou je leven kunnen veranderen. En als je je afvraagt of het verwerven van eeuwig inzicht *nuttig* is om in de wereld vooruit te komen? Er is een aardige anecdote over iemand die aan Euclides vraagt wat het *nut* is van het begrijpen van de stelling die juist wordt uitgelegd. Euclides wenkt zijn slaaf:

> Deze man wil graag zijn voordeel doen met wat hij hier leert. Zou je hem even een kwartje willen geven?

Eeuwige waarheid is alleen toegankelijk voor wie bereid is tot het geven van belangeloze aandacht.

1.2 Hoe krijg je (g)een hekel aan wiskunde?

Als je 's ochtends in trein of bus de *Spits* of *Metro* ter hand neemt zul je daar geen symbolen of afkortingen in tegenkomen waarvan je de betekenis niet weet. Zoiets stelt gerust. Van de *Spits* of *Metro* lezen word je niet moe. Ook in populair-wetenschappelijke boekjes komen (bijna) geen symbolen voor, ook al gaan ze over wiskunde of natuurkunde. Dat mag namelijk niet van de uitgevers. Elke formule halveert het aantal kopers, zo luidt de commerciële vuistregel.

Dit is echter een boek waarin niet alleen gezellig *over* wetenschap wordt gepraat, maar waarin ook echt wiskunde wordt *bedreven*, dus voor ons ligt de zaak noodzakelijkerwijs een tikkeltje anders. Wiskundigen gebruiken symbolen om mede-wiskundigen of wiskundigen-in-spe het leven gemakkelijker te maken. De symbolen zijn niet bedoeld om niet-wiskundigen af te schrikken.

Wat moet je doen als je toch schrikt van een onbegrijpelijke formule? Diep ademhalen tot je hartslag weer normaal is, en dan rustig kijken waar het wordt uitgelegd. Wetenschappelijke teksten geven hun geheimen pas bij geconcentreerd lezen prijs. Wiskundige bewijzen leren doorzien is een oefening in concentratie. Het is ook het "Sesam, open u!" naar één van de voor velen verborgen schatkamers van onze cultuur.

Als je twee dagen de *Spits* niet gelezen hebt maakt dat voor het begrijpen van de *Spits* van morgen niets uit, maar bij wiskunde ligt dat anders. Je kunt een hekel krijgen aan wiskunde als je niet door hebt dat elk nieuw wiskundig idee voortbouwt op eerdere ideeën. Om de draad te kunnen blijven vasthouden moet je je kennis voortdurend op peil houden. Eerst leer je vermenigvuldigen. Als je weet hoe dat moet weet je waarom $5 \times (22 + 33) = 5 \times 55 = 275$ en $5\times 22+5\times 33 = 110+165 = 275$ dezelfde uitkomst hebben. Als je daar vertrouwd mee bent leer je dat je kunt abstraheren van de getallen die je vermenigvuldigt door het gebruik van letters. Dan leer je dat het ervaringsfeit dat de uitkomst van $5\times(22+33)$ op twee verschillende manieren kan worden uitgerekend een voorbeeld is van de distributiewet $x(y + z) = xy + xz$. Als je zulke wetten begrijpt kun je leren wat vergelijkingen zoals $x = \frac{1}{1-x}$ betekenen. Vervolgens leer je hoe je zulke vierkantsvergelijkingen moet oplossen. Uiteindelijk snap je waarom de gulden snede gelijk is aan $\frac{1+\sqrt{5}}{2}$ (zie bladzijde 32).

Ieder nieuw stapje bouwt voort op eerdere stapjes, en op vaardigheden die je met die stapjes hebt ontwikkeld. Als je die vaardigheden paraat hebt is het zetten van het volgende stapje

meestal niet zo moeilijk. Als dat niet zo is zul je merken dat je het volgende stapje nauwelijks kunt zetten, omdat je het idee dat er achter zit maar half begrijpt. Bij het stapje dat daar op volgt ben je de draad dan helemaal kwijt. Op die manier raakt de lol er gauw vanaf, vooral als je ziet dat anderen totaal geen moeite hebben om te begrijpen wat er gebeurt.

1.3 De wortel uit 2 is geen breuk

De oude Grieken waren dol op constructies met behulp van passer en liniaal. Meetkunde gaat over cirkels en lijnen; cirkels teken je met een passer en lijnen trek je met een liniaal. Met een passer valt het middelpunt van een lijnstuk te bepalen, of kan een hoek middendoor worden gedeeld.

Opdracht 1.2 *Laat zien hoe je met passer en liniaal een gegeven hoek middendoor kunt delen.*

Opdracht 1.3 *Laat zien hoe je met passer en liniaal een loodlijn kunt construeren in een punt P op een lijn l. De loodlijn moet lijn l in P snijden onder een hoek van $90°$ (een rechte hoek). De benaming* loodlijn *is ontleend aan het 'loodkoord' waarmee een metselaar ervoor zorgt dat het muurtje dat hij aan het metselen is precies vertikaal is.*

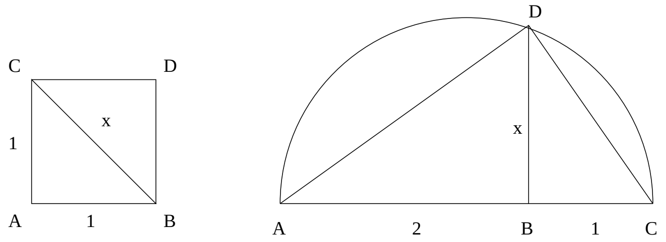
Opdracht 1.4 *De middelloodlijn van lijnstuk AB is de lijn die door het midden van het lijnstuk AB gaat en loodrecht op AB staat. Laat zien hoe je met behulp van een passer en een liniaal de middelloodlijn van een lijnstuk kunt construeren.*

Hoewel het liniaal van de oude Grieken geen schaalverdeling had, kunnen we wel een eenheidsmaat *afspreken*. We passen dan een of andere lengte af met de passer, en spreken af dat we die lengte 1 noemen. Dat is dan de afgesproken eenheidsmaat.

Bij een driehoek met een rechte hoek en rechthoekszijden van lengte 1 geldt volgens de stelling van Pythagoras (pagina 7) dat het kwadraat van de schuine zijde gelijk is aan 2 (twee maal de eenheidsmaat). Als we de schuine zijde x noemen wil dit zeggen: $x^2 = 2$.

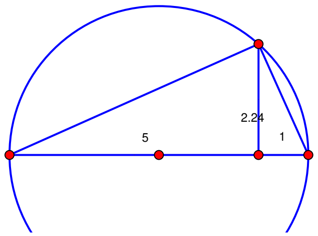
Met passer en liniaal valt een vierkant te construeren met zijde 1. Neem daartoe een lijnstuk AB en noem de lengte van dat lijnstuk 1. We hebben geen liniaal met schaalverdeling, maar we kunnen wel de lengte van AB als de eenheidsmaat beschouwen van een schaal die we zelf construeren. Noem de lijn die door A en B gaat l. Richt nu loodlijnen op l op in de punten A en B. Bepaal met een passer twee punten C en D op die loodlijnen, elk aan dezelfde kant van l, en op afstand 1 van respectievelijk A en B. Trek het lijnstuk CD en klaar is het vierkant. Trek de diagonaal CB in dit vierkant en noem de lengte x.

Een andere manier om x met $x^2 = 2$ te construeren is door te beginnen met twee lijnstukken AB en BC op dezelfde lijn, waarbij AB lengte 2 heeft en BC lengte 1. Construeer nu een halve cirkel met AC als diameter. Dat doe je door eerst het midden M van AC te bepalen, en dan vanuit dat midden met de passer een halve cirkel met straal AM te tekenen. Richt vanuit B een loodlijn op AC op, en noem het snijpunt van die loodlijn met de halve cirkel D. We laten straks zien dat $BD^2 = 2$. Omdat ADC een ingeschreven driehoek is van een cirkel met AC als diameter, geldt dat $\angle ADC$ een rechte hoek is. Dit is de cirkelstelling van Thales (opdracht 1.5).



Figuur 1.2: Twee manieren om $\sqrt{2}$ te construeren.

Het is nu gemakkelijk in te zien dat de driehoeken ADC, DBC en ABD in Figuur 1.2 gelijkvormig zijn. Uit de gelijkvormigheid van DBC en ABD volgt dat $AB : BD = BD : BC$. Dus is $AB \times BC = BD^2$, dat wil zeggen, $BD^2 = 2$. Deze constructie wordt beschreven in Euclides' *Elementen*, boek VI, Stelling 13. Het mooie van de constructie is dat het je in staat stelt een x met $x^2 = a$ te construeren voor elke gegeven lengte a: neem een lijnstuk AB van lengte a en een lijnstuk BC van lengte 1 en voer de constructie uit. Op de internetpagina bij dit boek vind je een bestand `Worteltrekken.html` dat deze constructie aanschouwelijk maakt (zie ook Figuur 1.3).



Figuur 1.3: Meetkundige constructie van $\sqrt{5}$.

Constructies met passer en liniaal zijn elementair en van een bijzondere schoonheid. De oude Grieken geloofden ook in de schoonheid van simpele verhoudingen. Als een strak gespannen snaar wordt verdeeld in stukken die zich verhouden als 1:2 of 2:3 of 3:4 of 4:5 dan zijn de tonen die je krijgt door die twee snaarstukken te tokkelen of aan te strijken in samenklank met elkaar en klinkt er een harmonisch interval (bij 1:2 een oktaaf, bij 2:3 een kwint, bij 3:4 een kwart, bij 4:5 een grote terts, bij 5:6 een kleine terts). Dit komt omdat bij dezelfde snaardikte en snaarspanning een twee keer zo lange snaar twee keer zo langzaam trilt, maar dat wisten de Grieken nog niet. De snaarverhoudingen $a : b$ corresponderen dus met verhoudingen van trillingsfrequenties $b : a$.

Stapelingen geven harmonische drieklanken. Zo levert de frequentieverhouding 4:5:6 een grote terts accoord op. De buitenste twee tonen staan in verhouding 4:6 of 2:3, dus ze vormen een kwint, de laagste twee vormen samen een grote terts, en de hoogste twee vormen samen een kleine terts. Voor Pythagoras en zijn leerlingen, die deze verhoudingen ontdekten, illustreerde dit dat de kosmos geordend is door eenvoudige getalsverhoudingen. Alle mooie verhoudingen zijn eenvoudige breuken.

Verhoudingen zijn direct verbonden met breuken. De breuken zijn alle getallen van de vorm $\frac{p}{q}$, waarbij p en q gehele getallen zijn, en de noemer q ongelijk is aan 0. We duiden de verzameling van alle breuken aan met $\mathbb{Q}$. Dit heet ook wel de verzameling van *rationale getallen* (getallen die een *ratio* of *verhouding* aangeven). We schrijven een breuk $\frac{p}{q}$ ook wel als p/q. Zo'n breuk drukt eigenlijk de verhouding $p : q$ uit.

Tot hun verbijstering ontdekten Griekse wiskundigen op zeker ogenblik dat sommige van de lijnstukken die je met passer en liniaal kunt construeren een lengte hebben die niet als breuk valt uit te drukken. We zagen zoëven dat je een rechthoekige gelijkbenige driehoek met rechthoekszijde 1 en schuine zijde x, met passer en liniaal kunt construeren. Maar x is geen breuk:

Stelling 1.1 *Er bestaat geen breuk x met $x^2 = 2$.*

Bewijs. Neem aan dat er een breuk x bestaat met $x^2 = 2$. Zo'n breuk heeft een teller m en een noemer n, met m en n allebei natuurlijke getallen, en de noemer n ongelijk aan 0.

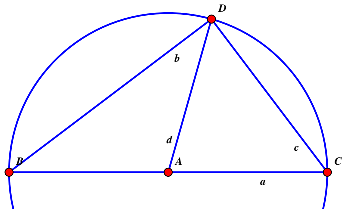
We mogen aannemen dat de breuk m/n niet verder te vereenvoudigen is, dat wil zeggen, m en n hebben geen gemeenschappelijke factoren. Preciezer: er zijn geen natuurlijke getallen k, p, q met $k \neq 1$, $m = kp$ and $n = kq$.

De breuk 2/10 kan worden vereenvoudigd, want de teller en noemer hebben een factor 2 gemeenschappelijk. Deze breuk kan door deling door 2 op eenvoudigste vorm worden gebracht: 1/5. Teller en noemer hebben nu geen gemeenschappelijke factoren meer.

Goed, we nemen aan dat $x = m/n$, met m en n zonder gemeenschappelijke factoren. Dan geldt: $x^2 = (m/n)^2 = 2$. Dus: $2 = (m/n)^2 = m^2/n^2$, en door beide zijden met n^2 te vermenigvuldigen vinden we: $2n^2 = m^2$. Met andere woorden: m^2 is even. Omdat kwadraten van oneven getallen altijd oneven zijn (immers, $(2n+1)^2 = 4n^2 + 4n + 1$ is oneven) moet m even zijn. Er is dus een natuurlijk getal p met $m = 2p$.

Invullen van $2p$ voor m in $2n^2 = m^2$ geeft $2n^2 = (2p)^2 = 4p^2$. Hieruit blijkt dat $n^2 = 2p^2$, en dat leidt weer tot de conclusie dat n ook even is. Maar dat betekent dat er een natuurlijk getal q is met $n = 2q$. Dit brengt ons in tegenspraak met de aanname dat m/n een breuk is in eenvoudigste vorm: we hebben immers een gemeenschappelijke factor 2 gevonden. Hieruit volgt dat er geen breuk x is met $x^2 = 2$, dat wil zeggen: de vierkantswortel uit 2 is geen breuk. ∎

De bewering die in Stelling 1.1 wordt bewezen heeft de vorm van een ontkenning: het is *niet* zo dat de wortel uit 2 een breuk is. Die ontkenning wordt aangetoond door aan te nemen dat er *wel* zo'n breuk is. Uit die aanname wordt vervolgens een tegenspraak afgeleid. Later, in hoofdstuk 5, zullen we de schematische vorm van dit bewijs verder bespreken. Nu je weet hoe een bewijs eruit ziet, kun je zelf proberen er een te leveren.



Figuur 1.4: De cirkelstelling van Thales

Opdracht 1.5 *Bewijs de stelling van Thales: "Een driehoek die door een halve cirkel wordt omschreven is een rechthoekige driehoek." Zie Figuur 1.4. Zie ook* `Thales.html` *op de website bij dit boek.*

We hebben hierboven laten zien dat er getallen zijn die niet als breuk te schrijven zijn. Zulke getallen heten *irrationale* getallen. De verzameling van alle rationale en irrationale getallen samen duiden we aan met $\mathbb{R}$. Dit heet de verzameling van *reële* getallen. Verderop in dit boek zullen vragen aan de orde komen zoals: "Hoeveel rationale getallen zijn er?" "Zijn dat er meer dan de natuurlijke getallen?" "Hoeveel reële getallen zijn er?"

1.4 Er zijn oneindig veel priemgetallen

Ons tweede voorbeeld van een beroemd bewijs is het bewijs dat er oneindig veel priemgetallen bestaan. Hopelijk herinner je je nog dat een priemgetal een natuurlijk getal is dat ongelijk is aan 1 en dat slechts deelbaar is door zichzelf en door 1. Voorbeelden van priemgetallen zijn 2 (deelbaar door 2 en door 1), 13 (deelbaar door 13 en door 1), 31 (deelbaar door 31 en door 1). Het getal 10 is geen priemgetal: het is deelbaar door 10, 5, 2 en 1. Volgens afspraak is 1 geen priemgetal.

Priemgetallen zijn de atomen waaruit natuurlijke getallen zijn opgebouwd, want elk natuurlijk getal groter dan 0 — elk getal uit de lijst $1, 2, 3, 4, \dots$ — kan worden ontleed in priemgetallen (of: 'ontbonden in priemfactoren'). Het getal 84 is gelijk aan $2 \times 2 \times 3 \times 7$, het getal 12345 kan worden geschreven als $3 \times 5 \times 823$, enzovoort. Het getal 823 is een priemgetal, dus het kan niet verder worden ontbonden. 'Hoeveel priemgetallen zijn er eigenlijk?' is dus een buitengewoon fundamentele vraag.

De stelling is van de vorm "Het is *niet* zo dat er slechts eindig veel priemgetallen bestaan." Als we het stramien van het bewijs van Stelling 1.1 zouden volgen zouden we het bewijs dus beginnen met de aanname: "Veronderstel dat er slechts eindig veel priemgetallen bestaan, zeg $2, 3, 5, 7, \dots, P$, waarbij P het grootste priemgetal is." Een bewijs volgens dit schema is inderdaad mogelijk. Het is echter ook mogelijk een direct bewijs te leveren. Dit doen we door de

N	$Q = N! + 1$	kleinste deler van Q groter dan N
2	3	3
3	7	7
4	25	5
5	121	11
6	721	7
7	5041	71
8	40321	61
9	362881	19
10	3628801	11
11	39916801	39916801
12	479001601	13
13	6227020801	83
14	87178291201	23
15	1307674368001	59
16	20922789888001	17
17	355687428096001	661
18	6402373705728001	19
19	121645100408832001	71
20	2432902008176640001	20639383
21	51090942171709440001	43
22	1124000727777607680001	23
23	25852016738884976640001	47
24	620448401733239439360001	811
25	15511210043330985984000001	401
26	403291461126605635584000001	1697
27	10888869450418352160768000001	?

Figuur 1.5: Tabel van priemgetallen groter dan N.

stelling te herformuleren als: "Voor elk natuurlijk getal N geldt dat er een priemgetal is dat groter is dan N." Het voordeel van deze aanpak is dat het bewijs ons nu in principe een procedure (wiskundigen en informatici zeggen: een *algoritme*) levert om aan een priemgetal groter dan N te komen.

We zeggen dat een natuurlijk getal N een natuurlijk getal M deelt als de deling van M door N geen rest oplevert. In zo'n geval is er dus een natuurlijk getal K met $M = N \times K$.

Stelling 1.2 *Er zijn oneindig veel priemgetallen.*

Bewijs. We laten zien dat er voor elk natuurlijk getal N een priemgetal moet bestaan dat groter is dan N. Laat N gegeven zijn. Beschouw nu het getal $Q = N! + 1$. Voor wie de definitie van $N!$ ("N faculteit") vergeten is:

$$Q = (1 \times 2 \times 3 \times 4 \times 5 \times \cdots \times N) + 1.$$

Nu gaan we met behulp van Q systematisch op zoek naar een priemgetal dat groter is dan N. Dat doen we door de volgende probeermethode toe te passen. We lopen de getallen $N+1$, $N+2$, $N+3, \ldots$, langs en proberen uit of dit getal Q deelt (gewoon, door de deling uit te voeren en de kijken of de rest 0 wordt). Vroeg of laat vinden we op deze manier een getal P met de volgende eigenschappen:

- P deelt Q, dat wil zeggen: er is een A met $Q = P \times A$.
- geen getal tussen N en P deelt Q.

De garantie dat we zo'n P zeker vinden zit hem in het feit dat Q zichzelf deelt.

De P die we op deze manier vinden is een priemgetal. Immers, Q is zo gekozen dat voor alle priemgetallen kleiner dan of gelijk aan N geldt dat ze Q niet delen. Ze geven immers rest 1 bij deling op Q. Als P zelf opgebouwd zou zijn uit kleinere priemfactoren dan zouden die dus elk groter dan N moeten zijn, en dan zouden we ze al gevonden moeten hebben. ∎

N	$Q =$ (product van alle priemgetallen $\leq N) + 1$	kleinste deler van Q groter dan N
2	3	3
3	7	7
4	7	7
5	31	31
$\vdots$	$\vdots$	$\vdots$
26	223092871	317
27	223092871	317
28	223092871	317
29	6469693231	331
30	6469693231	331
31	200560490131	?

Figuur 1.6: Tabel van priemgetallen groter dan N.

Goed, we hebben nu een procedure voor het vinden van grote priemgetallen. Een computer kan dan het werk voor ons doen, zou je zeggen. In principe is dat juist, maar in de praktijk blijkt dat zelfs de krachtigste computer stuk loopt op dit algoritme. Om dit te illustreren kijken we even naar een paar kleine waarden voor N. De tabel in Figuur 1.5 maakt heel duidelijk hoe gruwelijk dit uit de hand gaat lopen.

Opdracht 1.6 *(Voor wie kan programmeren:) Schrijf een programma in je favoriete programmeertaal dat als invoer een natuurlijk getal N neemt en als uitvoer een priemgetal groter dan N oplevert. Probeer met dit programma uit voor welke N je nog binnen redelijke tijd een antwoord krijgt.*

Nu zou je kunnen zeggen dat de keuze van Q als $N! + 1$ nodeloos groot is. Voor het bewijs is het immers voldoende om het product te nemen van alle *priemgetallen* kleiner of gelijk aan N, en daar 1 bij op te tellen. Dit is juist, maar het lost de moeilijkheid niet op. Ook dit loopt gruwelijk uit de hand. Kijk maar naar de tabel in Figuur 1.6.

1.5 Over de schoonheid en het nut van wiskunde

In een bekend pleidooi voor het bedrijven van wiskunde als doel op zichzelf [12] neemt de Engelse wiskundige G.H. Hardy de bewijzen van de twee stellingen die we zojuist hebben gepresenteerd als schoolvoorbeelden van mooie en diepe bewijzen. Hardy probeert vervolgens te omschrijven waarom deze stellingen, met hun bewijzen, zoveel mooier zijn dan de puzzels die je bij voorbeeld in breinbrekerboekjes vindt. Wat deze twee stellingen zoveel dieper maakt dan het eerste het beste schaakprobleem, zegt Hardy, is dat ze het denken diepgaand beïnvloed hebben terwijl het voor ons denken niet zoveel zou hebben uitgemaakt als het schaken nooit zou zijn uitgevonden.

Neem de stelling dat er oneindig veel priemgetallen zijn. De priemgetallen vormen het ruwe materiaal waaruit elk natuurlijk getal is opgebouwd, en daarmee vormen ze de grondstof van het rekenen. De stelling vertelt ons niets meer of minder dan dat de grondstof voor het rekenen niet kan worden uitgeput.

Wat de stelling over de irrationaliteit van wortel 2 ons vertelt is dat de prachtige theorie van het rekenen die we met behulp van onze oneindige voorraad priemgetallen hebben opgebouwd nooit genoeg zal zijn, omdat er grootheden zijn die zich direct aan ons opdringen en die we er *niet* mee zullen kunnen meten. De Griekse wiskundigen zagen het fundamentele belang van dit inzicht direct in. De ontdekking van de irrationale getallen leidde tot een diepe theorie over verhoudingen, de theorie van Eudoxos (opgenomen in boek V van Euclides' *Elementen*).

Hardy gaat dan verder met de opmerking dat beide stellingen geen enkel praktisch nut hebben. Hij merkt venijnig op dat er 50 847 478 priemgetallen zijn die kleiner zijn dan een miljard, en voor een ingenieur is dat meer dan genoeg. Ook aan irrationale getallen hebben praktisch ingestelde mensen geen boodschap:

> [...] het is duidelijk dat irrationale getallen oninteressant zijn voor een ingenieur, want die heeft genoeg aan een benadering, en alle benaderingen zijn breuken.

Dit valt gemakkelijk te illustreren aan een concreet voorbeeld. In de grafische industrie bestaat er een industrienorm (DIN) voor papierformaten A0, A1, A2, A3, A4, A5 en A6. De bedoeling van die formaten is dat je een A1 vel krijgt door een A0 vel dubbel te vouwen (of dat je twee A1 vellen krijgt door een A0 vel doormidden de snijden), een A2 vel door een A1 vel dubbel te vouwen, enzovoort. Er gaan dus 16 velletjes A4 uit een vel A0. De maten zijn zo vastgesteld dat de verhoudingen tussen lange zijde z en korte zijde k bij dubbelvouwen behouden blijven. Die verhouding wordt dus gegeven door $z : k = 2k : z$. Korte zijde gelijk stellen aan 1 geeft: $z = \frac{2}{z}$, dat wil zeggen $z = \sqrt{2}$. De lange zijde staat dus tot de korte zijde als $\sqrt{2}$ staat tot 1. Op websites waar de verhouding tussen lange en korte zijde van papierformaten worden uitgelegd wordt echter steevast gesproken van de verhouding 7 staat tot 5.

Met zijn bewering, gedaan in 1940, dat zuivere wiskunde geen enkel praktisch nut heeft heeft Hardy overigens groot ongelijk gekregen. Juist het feit dat de rekenkunde procedures kent die ook met de krachtigste computer ondoenlijk zijn omdat de berekening simpelweg teveel tijd kost, terwijl de omgekeerde procedure met behulp van een computer een fluitje van een cent is bleek de sleutel tot een zeer belangrijke toepassing, de zogenaamde publieke sleutel cryptografie (*public key cryptography*). Twee heel grote priemgetallen met elkaar vermenigvuldigen is met een computer heel gemakkelijk. Maar als P en Q twee heel grote priemgetallen zijn, dan is het vrijwel onbegonnen werk om die factoren terug te vinden uit het product $P \times Q$. Er bestaan wel iets betere methoden dan ruwweg systematisch uitproberen van mogelijkheden, maar echt helpen doet dat (nog) niet.

Als je geld wilt pinnen en je tikt je pincode in, dan stuurt de pinautomaat niet die pincode door ter controle, maar in plaats daarvan een zeer groot getal A dat aan de pincode is gekoppeld. Dat getal A is een product van twee zeer grote priemgetallen P en Q, maar die twee getallen staan *niet* op de pinpas, en ze kunnen ook *niet* worden afgeleid uit de pincode. Het getal A kan wel uit de pinpas gecombineerd met de pincode worden afgeleid. Iemand zou nu het electronische verkeer tussen de pinautomaat en de bank kunnen onderscheppen en het getal A te weten kunnen komen dat door de pinautomaat wordt doorgestuurd naar de bank. Maar zo iemand heeft daar niets aan. Alleen de instantie die de pinpassen heeft versterkt beschikt over de P die hoort bij de A van jouw pinpas plus pincode. Die instantie voert de deling A/P uit en krijgt als uitkomst een rest 0. Wie die P niet heeft kan niets met A beginnen, want ontbinden van het getal A in priemfactoren kost, met alle wiskundige technieken die daar nu voor bekend zijn, astronomisch veel tijd.

Zuivere wiskunde blijkt nauw verweven met wereldse zaken als de beveiliging van ons girale geldverkeer, en nieuwe inzichten uit de zuivere wiskunde zouden de manier waarop banken wereldwijd functioneren in gevaar kunnen brengen. De ontdekking van een zeer efficiënte methode om grote getallen te ontbinden in priemfactoren zou het maatschappelijk verkeer dus behoorlijk kunnen ontwrichten. Dat zo'n wetenschappelijke doorbraak geen puur theoretische mogelijkheid is blijkt uit het volgende voorbeeld. Eeuwenlang hebben wiskundigen gezocht naar een praktisch uitvoerbare en waterdichte methode om te testen of een getal een priemgetal is. Een waterdichte methode om uit te vinden of N een priemgetal is gaat als volgt: probeer eerst of 2 een deler is, vervolgens of 3 een deler is, en zo verder voor alle natuurlijke getallen $\leq \sqrt{N}$. Deze methode is echter voor zeer grote getallen N niet praktisch bruikbaar, want ze vergt astronomisch veel tijd. Praktisch bruikbare methoden waren wel bekend, maar die waren juist niet waterdicht: ze boden geen absolute zekerheid dat een getal dat door de test kwam ook echt priem was. In 2002 werd er tot grote verrassing van de wetenschappelijke wereld door drie wiskundigen uit India[1] een methode gevonden die zowel praktisch uitvoerbaar als waterdicht is.

[1] Agrawal, Kayal en Saxena

Hoofdstuk 2

(In)zien en Bewijzen

2.1 Natuurlijke Getallen en Volledige Inductie

In deze eerste paragraaf voeren we een belangrijke bewijsmethode in. Zoals we later zullen zien levert deze methode wel altijd zekerheid maar niet altijd inzicht.

De natuurlijke getallen zijn $0, 1, 2, 3, 4, 5, \ldots$. We duiden de verzameling van alle natuurlijke getallen aan met $\mathbb{N}$. De natuurlijke getallen zijn fundamenteel voor het aftellen van eindige hoeveelheden dingen. Verderop in dit boek zullen we zien dat de natuurlijke getallen ons in de steek laten bij het aftellen van oneindige hoeveelheden.

Het is gebruikelijk het getal 0 bij de natuurlijke getallen te rekenen. Het heeft overigens tot in de Renaissance geduurd voor wiskundigen zich enigszins op hun gemak voelden met het getal 0. Indiase wiskundigen rekenden al voor het begin van onze jaartelling met 0, maar de oude Grieken beschouwden 0 niet als een getal. Het getal 0 is handig voor positionele getalnotatie (de 1 in 10 heeft een andere waarde dan de 1 in 1000, vanwege de andere positie). Positionele getalnotatie was iets dat de Grieken niet hadden, maar de Babyloniërs weer wel. Bij de Babyloniërs was de positionele getalnotatie echter dubbelzinnig. Juist omdat zij het getal 0 niet hadden maakten ze aanvankelijk geen onderscheid tussen (bij voorbeeld) 216 en 2106.

Aan het eind van de Middeleeuwen beschreef de Italiaan Leonardo Fibonacci (1170–1250) de negen Indiase symbolen voor wat wij nu de 'arabische cijfers' noemen (de positionele getalnotatie was ook in India uitgevonden, en van daar door Arabieren in Europa geïmporteerd), plus het symbool voor nul. Interessant genoeg introduceert hij $1, 2, 3, 4, 5, 6, 7, 8, 9$ als 'getallen', maar noemt hij 0 een 'teken'. Helemaal lekker zat dit nieuwe getal hem kennelijk nog niet.

Je kunt je de natuurlijke getallen als volgt voorstellen:

- Het getal 0 is gegeven.
- Als je bij een getal n bent aangekomen, dan is er altijd een volgend getal, namelijk $n + 1$, het getal dat je krijgt door 1 bij n op te tellen.
- Er is geen natuurlijk getal dat je niet in een eindig aantal stappen vanaf 0 kunt bereiken.

Het feit dat je elk natuurlijk getal in een eindig aantal stappen vanaf 0 kunt bereiken maakt het mogelijk om beweringen van de vorm "Voor elk natuurlijk getal n geldt dat ..." met behulp van *volledige inductie* te bewijzen. Het bewijsstramien van een bewijs met volledige inductie is als volgt:

Te bewijzen: Voor elk natuurlijk getal n geldt de eigenschap E.

Bewijs:

Basisgeval Voor 0 geldt E want ...

Inductiestap Stel dat voor n de eigenschap E geldt.

Te bewijzen: Voor $n + 1$ geldt de eigenschap E.

Bewijs: ...

Je bewijst dus dat E aan het begin van de oneindige lijst van natuurlijke getallen geldt, en vervolgens laat je zien dat, als je bij zeker getal in de oneindige lijst van natuurlijke getallen E hebt, je E ook hebt voor het daaropvolgende getal. Het is duidelijk dat je op deze manier E van elk natuurlijk getal kan laten zien.

Informeler gezegd komt volledige inductie hierop neer: je wilt oneindig veel beweringen bewijzen, en je doet dit door te laten zien dat bewering B_0 waar is, en dat elke bewering B_n in de oneindige rij de bewering B_{n+1} impliceert.

Wellicht heb je hier bij de wiskundelessen al voorbeelden van gezien. Ook in dit boek zul je dit bewijsstramien een aantal malen tegenkomen.

Als voorbeeld van hoe je iets met volledige inductie bewijst beschouwen we het volgende lucifersspelletje voor twee spelers. Spelsituatie: er ligt een hoopje lucifers op tafel. De spelers A en B zijn om beurten aan zet. De toegestane zetten in het spel zijn:

- één lucifer van tafel nemen,
- twee lucifers van tafel nemen,
- drie lucifers van tafel nemen.

De speler die als laatste een toegestane zet kan doen heeft gewonnen.

Als A aan zet is in een situatie met 3 lucifers op tafel heeft A gewonnen: A neemt dan gewoon alle lucifers en B kan niets meer doen. Net zo voor een situatie met 2 lucifers op tafel of met 1 lucifer op tafel.

Experimenteel is al snel in te zien dat een speler altijd kan winnen als de tegenspeler aan zet is terwijl het aantal lucifers op tafel een viervoud is. We laten nu met volledige inductie naar n zien dat A altijd kan winnen als B aan zet is in een situatie met $4n$ lucifers op tafel.

Basisgeval: Als $n = 0$ dan liggen er dus $4n = 0$ lucifers op tafel. B is aan zet en kan niets doen, dus A heeft gewonnen.

Inductiestap: Neem aan dat A kan winnen als er $4n$ lucifers op tafel liggen en B is aan zet. Dit is de inductiehypothese. Stel nu dat er $4(n + 1) = 4n + 4$ lucifers op tafel liggen, en B is aan zet. B kan drie dingen doen.

1. B neemt 1 lucifer. Dan neemt A 3 lucifers. B is weer aan zet, en er liggen $4n$ lucifers op tafel. Volgens de inductiehypothese kan A dit winnen.

2. B neemt 2 lucifers. Dan neemt A 2 lucifers. B is weer aan zet, en er liggen $4n$ lucifers op tafel. Volgens de inductiehypothese kan A dit winnen.

3. B neemt 3 lucifers. Dan neemt A 1 lucifer. B is weer aan zet, en er liggen $4n$ lucifers op tafel. Volgens de inductiehypothese kan A dit winnen.

Het is duidelijk dat A altijd kan winnen als B aan zet is terwijl er een viervoud aan lucifers op tafel ligt.

Overigens hoeft de inductie niet per se bij 0 of 1 te beginnen. De volgende opdracht is een voorbeeld met basisgeval $n = 5$.

Opdracht 2.1 *Laat met volledige inductie zien dat $2^n > n^2$ voor elk natuurlijk getal n met $n \geq 5$.*

Als je de bewering uit opdracht 2.1 zou proberen aan te tonen met basisgeval $n = 0$ (of $n = 1$, of $n = 2$, of $n = 3$, of $n = 4$) dan zou dat niet lukken.

2.2 Oefenen met Bewijzen

De eenvoudigste vorm van rekenen is het optellen en vermenigvuldigen met natuurlijke getallen. We definiëren nu het volgende begrip voor het rekenen met natuurlijke getallen. Als a en b natuurlijke getallen zijn zeggen we dat a deler is van b als er een natuurlijk getal N is met de eigenschap dat $aN = b$. Met andere woorden: als je b door a deelt krijg je uitkomst N, met rest 0. We korten "a is deler van b" af als $a|b$.

Hier is een eerste voorbeeld van een bewering over natuurlijke getallen die we gaan proberen te bewijzen. Bewijzen wil niets anders zeggen dan: laten zien waarom dit zo is.

Opdracht 2.2 *Laat zien: als a, b, c natuurlijke getallen zijn met $a|b$ en $b|c$, dan geldt ook $a|c$.*

De methode die je kunt toepassen: aannemen dat $a|b$ en $b|c$ allebei het geval zijn, en laten zien dat hieruit volgt dat $a|c$ ook het geval moet zijn.

De volgende twee opdrachten hebben betrekking op een functie die we definiëren met behulp van het begrip 'deler zijn van'. We spreken af dat KD een functie is van natuurlijke getallen naar natuurlijke getallen die elk natuurlijk getal n dat groter is dan 1 afbeeldt op de kleinste deler van n die ongelijk is aan 1. Bij voorbeeld, KD beeldt 2 af op 2, 3 op 3, 4 op 2, enzovoort. Met andere woorden: KD(n) is de kleinste deler van n. Dit wil zeggen dat KD(n) voldoet aan de volgende drie eisen (aangenomen dat n groter is dan 1):

1. $\mathrm{KD}(n) \neq 1$,

2. $\mathrm{KD}(n)|n$,

3. als $m|n$ en $m \neq 1$ dan $m \geq \mathrm{KD}(n)$.

Opdracht 2.3 *Laat zien: als $n > 1$ dan is $KD(n)$ een priemgetal. Hint: neem aan dat $n > 1$ en dat $KD(n)$* geen *priemgetal is, en laat zien dat die combinatie van aannamen een tegenspraak oplevert.*

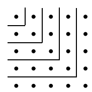
Opdracht 2.4 *Laat zien: als $n > 1$ en n is geen priemgetal, dan is $(KD(n))^2 \leq n$.*

De functie KD is nuttig bij het definiëren van een test om te kijken of een natuurlijk getal een priemgetal is: priemgetallen zijn de natuurlijke getallen n groter of gelijk aan 2 waarvoor geldt dat $\mathrm{KD}(n) = n$. De priem-test voor een getal n kan de vorm aannemen van systematisch zoeken naar een kleinste deler van n. Probeer eerst of 2 een deler is, vervolgens of 3 een deler is, en zo verder voor alle natuurlijke getallen $\leq \sqrt{n}$. Als dit geen deler oplevert is kennelijk $\mathrm{KD}(n) = n$, dat wil zeggen: n is priem.

2.3 Plaatjes en inzicht

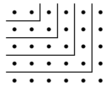
Als je iets direct 'ziet' hoef je het niet meer te bewijzen. Echt inzicht is fundamenteler dan bewijs. Sherlock Holmes zegt "elementair, beste vriend", maar voor Watson moet het inzicht nog worden uitgespeld door middel van uitgebreide bewijsvoering.

Vaak valt een direct inzicht te illustreren met een plaatje, en zo'n plaatje zegt dan meer dan een bewijs in woorden. Het volgende plaatje (dat je misschien al eens bij wiskunde hebt gezien) illustreert het inzicht dat de som van de eerste n oneven natuurlijke getallen gelijk is aan n^2. Het plaatje geeft de som $1 + 3 + 5 + 7 + 9$.



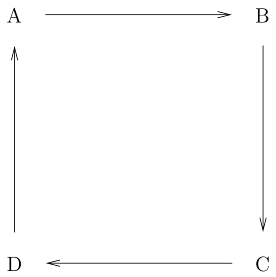
In feite geeft het plaatje natuurlijk alleen een speciaal geval. Het *inzicht* is nu juist dat je elk plaatje van zo'n speciaal geval kunt uitbreiden tot een plaatje van een groter vierkant door een nieuwe 'rand' van punten toe te voegen. Bij voorbeeld: een vierkant met 5×5 punten kun je uitbreiden tot een vierkant van 6×6 punten door een nieuwe 'rand' van 11 punten toe te voegen, en 11 is het zesde oneven getal. Een vierkant van 12×12 punten kun je uitbreiden tot een vierkant van 13×13 punten door het toevoegen van een nieuwe 'rand' van $2 \times 12 + 1 = 25$ punten. Algemener geformuleerd: je kunt een plaatje van $n \times n$ punten uitbreiden tot een plaatje van $(n+1) \times (n+1)$ punten door er een 'rand' van $2n+1$ punten aan toe te voegen. Dit inzicht is in feite de kern van de *inductiestap* in een bewijs met volledige inductie.

Opdracht 2.5 *Kun je uit het volgende plaatje van $2+4+6+8+10$ (de som van de eerste 5 even natuurlijke getallen) een formule destilleren voor de som van de eerste n even natuurlijke getallen? (Ook dit voorbeeld zou je je nog moeten herinneren uit de wiskundelessen.)*

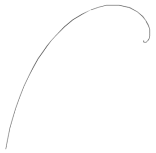


Hier is nog een voorbeeld waar direct inzicht beter werkt dan toepassen van wiskundige techniek.

Opdracht 2.6 *Raadsel van de verliefde kevers. Er waren eens vier kleine kevertjes, A, B, C en D, en die zaten niet op een hek, maar in de vier hoeken van een vierkant:*



A is verliefd op B, B is verliefd op C, C is verliefd op D en D is weer verliefd op A. De zijde van het vierkant heeft lengte a. Als de god Amor het startschot geeft beginnen de kevertjes te lopen. A loopt recht op B af, B loopt recht op C af, C loopt recht op D af, en D loopt recht op A af. Ieder kevertje blijft het kevertje waar hij verliefd op is in het oog houden en blijft er recht op af lopen. De kevertjes lopen alle vier met constante snelheid, en even snel. Vraag: komen de kevertjes elkaar ooit tegen? Zo ja, welke afstand hebben ze afgelegd als ze elkaar ontmoeten? Hier is de weg van het kevertje dat linksonder vertrekt:



Wie de kevertjes puzzle leuk vindt zal ook plezier hebben aan de volgende vraag.

Opdracht 2.7 *Twee goederentreinen rijden op elkaar af op hetzelfde spoor. Ze zijn tweehonderdvijftig kilometer van elkaar verwijderd. De eerste trein rijdt 110 kilometer per uur, de tweede 140 kilometer per uur. Een turbovlieg vliegt tussen de twee locomotieven heen en weer, met 200 kilometer per uur, tot ze op elkaar botsen. Welke afstand heeft de turbovlieg afgelegd op het moment dat hij tussen de twee locomotieven verpletterd wordt?*

Nog een opdracht die vraagt om inzicht. Als je het inzicht hebt kun je de 'waarom' vraag beantwoorden, en dan heb je dus ook een bewijs.

Opdracht 2.8 *In een vaas zitten 35 witte en 35 zwarte steentjes. Je gaat, zolang dat mogelijk is, als volgt te werk. Je haalt steeds twee steentjes uit de vaas. Als ze dezelfde kleur hebben stop je een zwart steentje terug in de vaas, als ze verschillende kleur hebben stop je het witte steentje terug in de vaas. Er zijn voldoende extra zwarte steentjes. Omdat er bij elke stap een steentje verwijderd wordt is er na 69 stappen nog maar één steentje over. Welke kleur heeft dat steentje? Waarom?*

2.4 Niet alle bewijzen geven (evenveel) inzicht

Hier volgen vijf bewijzen van $1+\cdots+n=\frac{n(n+1)}{2}$. Ga zelf na welk bewijs jou het meeste inzicht geeft.

Eerste bewijs:

Zet $1+\cdots+n$ in twee rijen onder elkaar:

$$\begin{array}{ccccccccc} 1 & + & 2 & + & \cdots & + & (n-1) & + & n \\ n & + & (n-1) & + & \cdots & + & 2 & + & 1 \end{array}$$

Tel nu kolomsgewijs op:

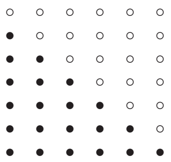
$$(n+1) \quad + \quad (n+1) \quad + \quad \cdots \quad + \quad (n+1) \quad + \quad (n+1)$$

Er zijn n kolommen, dus het resultaat van tweemaal de som $1+\cdots+n$ nemen is $n(n+1)$. Resultaat van eenmaal de som $1+\cdots+n$ nemen is dus gelijk aan $\frac{n(n+1)}{2}$.

Dit is de manier waarop Karl Gauss als zevenjarige scholier onmiddellijk inzag dat $1+2+3+\cdots+98+99+100$ gelijk is aan 5050.

Tweede bewijs:

Merk op dat de volgende rechthoek bestaat uit $n+1$ rijen van n kolommen, en dat de zwarte bolletjes precies de helft van de rechthoek vormen.



Derde bewijs:

Dit is een bewijs voor mensen die zich herinneren dat $\binom{n}{k}$ staat voor het aantal manieren waarop je k dingen kunt kiezen uit n mogelijkheden. De algemene formule voor $\binom{n}{k}$ is $\frac{n!}{k!\,(n-k)!}$. Zie bladzijde 14 voor de definitie van $n!$.

$\binom{n+1}{2} = \frac{n(n+1)}{2}$ geeft het aantal manieren om twee dingen te kiezen uit $n+1$ mogelijkheden. Waarom is dit nu gelijk aan $1 + \cdots + n$? Neem aan dat je een bak met $n+1$ knikkers hebt, genummerd van 1 tot en met $n+1$. Je neemt twee knikkers uit de bak, met de afspraak dat de tweede knikker een *lager* nummer moet hebben dan de eerste. Als je eerste knikker nummer k heeft kun je je tweede knikker op $k-1$ manieren kiezen; er zitten immers $k-1$ knikkers in de bak met een lager nummer dan k. Totaal geeft dit $1 + 2 + \cdots + n$ manieren om twee knikkers uit de bak te halen.

Vierde bewijs:

We hebben hierboven gezien (opdracht 2.5 op bladzijde 23) dat de som van de eerste n even getallen $n(n+1)$ is. Welnu, als je de eerste n even getallen neemt, en je deelt elk ervan door 2, dan krijg je de eerste n getallen. De som van de eerste n getallen is dus $\frac{n(n+1)}{2}$.

Vijfde bewijs:

Het vijfde bewijs is een inductiebewijs, naar het stramien van bladzijde 19. Bij een bewijs met inductie laat je twee dingen zien (we nemen even aan dat de inductie bij 1 begint):

1. Voor het geval $n = 1$ gaat de bewering op, en

2. als je aanneemt dat de bewering opgaat voor het geval n, dan kun je daaruit afleiden dat de bewering ook opgaat voor het geval $n+1$.

De aanname, in (2), dat de bewering opgaat voor n, heet de *inductie hypothese*. In het voorbeeldbewijs luidt de inductie hypothese: $1+\cdots+n = \frac{n(n+1)}{2}$. Die hypothese wordt vervolgens gebruikt in de stap die wordt aangegeven met $\stackrel{\text{ih}}{=}$.

Basisstap: voor $n = 1$ geldt dat $\frac{n(n+1)}{2} = 1$. Dit is inderdaad de som van de natuurlijke getallen tot en met 1.
Inductiestap. Neem aan (inductiehypothese) dat $1 + \cdots + n = \frac{n(n+1)}{2}$. We moeten nu aantonen:

$$1 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}.$$

Dit volgt direct uit:

$$1+\cdots+n+(n+1) \stackrel{\text{ih}}{=} \frac{n(n+1)}{2} + (n+1) = \frac{n^2+n}{2} + \frac{2n+2}{2} = \frac{n^2+3n+2}{2} = \frac{(n+1)(n+2)}{2}$$

Het nadeel van het inductiebewijs ten opzichte van de andere bewijzen is dat het aan het eind van het bewijs nog steeds een raadsel is hoe je de betrekking $1+\cdots+n = \frac{n(n+1)}{2}$ zelf zou kunnen vinden.

Als je de andere bewijzen met elkaar vergelijkt dan zie je dat ze steeds andere verbanden leggen. Een nieuw bewijs van iets dat je al hebt ingezien kan dus toch voor nieuw inzicht zorgen, doordat het nieuwe verbanden legt tussen dingen die je al weet.

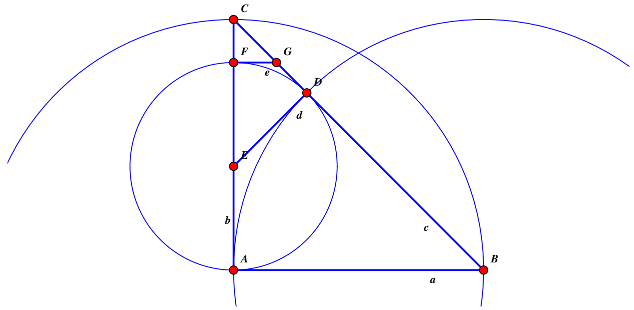
2.5 Meer bewijzen, meer inzicht

In het bewijs van Stelling 1.1 hebben we gezien dat de vierkantswortel van 2 geen breuk is. Dit feit kan ook op allerlei andere manieren worden ingezien. Hier is een meetkundig bewijs uit [14]. In dit bewijs wordt $|AB|$ gebruikt voor de *lengte* van het lijnstuk dat A met B verbindt.

Bewijs 2 van 'er bestaat geen breuk x met $x^2 = 2$'. Laat $\triangle ABC$ een gelijkbenige rechthoekige driehoek zijn. Zie Figuur 2.1. Dan is volgens de stelling van Pythagoras de verhouding tussen de lengten van de lijnstukken BC en AB gelijk aan $\sqrt{2}$. Stel nu dat dit gelijk zou zijn aan een breuk p/q. Dan zouden $|BC|$ en $|AB|$ allebei gehele veelvouden moeten zijn van een gemeenschappelijke maat m. Immers, stel $|AB| = q \cdot m$, dan is $|AB| = p \cdot m$.

Laat D het punt zijn op de hypothenusa BC dat bepaald wordt door $|BD| = |AB|$. Laat E het snijpunt zijn van de loodlijn op BC in D met AC. Dan geldt $|AE| = |ED| = |DC|$. Immers, $|AE| = |ED|$ omdat E het middelpunt is van de cirkel door A en D, en $|ED| = |DC|$ omdat $\triangle DCE$, wegens gelijkvormigheid met $\triangle BAC$, een gelijkbenige rechthoekige driehoek is.

Dus zijn $|CD| = |BC| - |AB|$ en $|EC| = |AC| - |AE| = |AB| - (|BC| - |AB|)$ allebei gehele veelvouden van m (omdat $|AB|$ en $|AC|$ dat zijn).



Figuur 2.1: Meetkundig bewijs van de irrationaliteit van $\sqrt{2}$.

Nu kunnen we deze hele redenering herhalen voor de driehoek $\triangle EDC$. Laat $|EF| = |ED|$, en laat de loodlijn op EC in F het lijnstuk DC snijden in G. Dan zijn $|FG|$ en $|GC|$ allebei gehele veelvouden van m (omdat $|ED|$ en $|EC|$ dat zijn).

Deze procedure kan willekeurig vaak worden herhaald. Dit geeft een rij van lengten van lijnstukken $|AC|$,$|EC|$, $|FC|$ met de eigenschap dat elk ervan een geheel veelvoud van m is. Maar dan vormt de corresponderende rij van positieve gehele getallen een monotoon dalende rij, en dat is onmogelijk. Een monotoon dalende reeks van getallen is een reeks waarbij elk volgend getal kleiner is dan zijn voorganger. Elke monotoon dalende rij van positieve gehele getallen moet eindig zijn, want vanaf elk positief geheel getal kun je in eindig veel stappen terugtellen naar 0. ∎

Uit het bovenstaande meetkundige bewijs valt een algebraïsch bewijs te destilleren, als volgt. Beschouw nogmaals Figuur 2.1. Laat $|BC| = p$ en $|AB| = q$. Dan geldt dat $|EC| = |AB| - (|BC| - |AB|) = 2|AB| - |BC| = 2q - p$. Ook geldt $|ED| = |BC| - |AB| = p - q$. Op grond van wat we net meetkundig hebben ingezien volgt nu: $(2q - p)/(p - q) = p/q = \sqrt{2}$.

We laten nu de irrationaliteit van $\sqrt{2}$ zien met behulp van algebra, waarbij we de meetkunde elimineren:

Bewijs 3 van '$\sqrt{2}$ is geen breuk'. Neem aan dat $\sqrt{2} = p/q$, waarbij p en q positieve natuurlijke getallen zijn, met q zo klein mogelijk. Dan hebben we:

$$\frac{2q-p}{p-q} = \frac{2-(p/q)}{(p/q)-1} = \frac{2-\sqrt{2}}{\sqrt{2}-1} = \frac{(2-\sqrt{2})(\sqrt{2}+1)}{(\sqrt{2}-1)(\sqrt{2}+1)} = \sqrt{2} = \frac{p}{q}.$$

Omdat $2q - p$ en $p - q$ gehele getallen zijn met $0 < p - q < q$, is dit in tegenspraak met de minimaliteit van q. ∎

Het meetkundige en het algebraïsche bewijs zien er op het eerste oog misschien heel verschillend uit, maar ze zijn in de kern hetzelfde.

Tenslotte een alternatief bewijs voor de oneindigheid van de verzameling priemgetallen, uit een brief van Christian Goldbach aan Leonhard Euler uit 1730 [1]. Het bewijs maakt gebruik van de reeks van zogenaamde Fermat getallen $F_n = 2^{2^n} + 1$, voor $n = 0, 1, 2, \ldots$.

Opdracht 2.9 *Reken de Fermat getallen F_0, F_1, F_2, F_3 en F_4 uit.*

Het is gemakkelijk na te gaan dat F_0, F_1, F_2, F_3 priemgetallen zijn. Pierre de Fermat (1601–1665) slaagde er in om te laten zien dat ook F_4 een priemgetal is. Fermat sprak op grond van het feit dat F_0, F_1, F_2, F_3, F_4 allemaal priem zijn het vermoeden uit dat elke getal van de vorm $2^{2^n} + 1$ een priemgetal is. Leonard Euler slaagde er in 1732 in om F_5 in factoren te ontbinden, met als uitkomst $F_5 = 4294967297 = 641 \cdot 6700417$. Geen priemgetal. Voor F_6 geeft de computer de uitkomst $F_6 = 18446744073709551617 = 274177 \cdot 67280421310721$. Ook geen priemgetal.

Opdracht 2.10 *(Voor wie kan programmeren.) Gebruik de computer en je favoriete programmeertaal om nog een aantal getallen uit de Fermat reeks uit te rekenen. Lukt het ook om na te gaan welke van die getallen priem zijn en welke niet?*

Goed, hier komt Goldbachs bewijs van de oneindigheid van de verzameling priemgetallen.

Bewijs 2 van de oneindigheid van de verzameling priemgetallen. Beschouw de reeks van Fermat getallen $F_n = 2^{2^n} + 1$, voor $n = 0, 1, 2, \ldots$. Als we kunnen laten zien dat elk volgend Fermat getal bestaat uit priemfactoren die in geen van de eerdere Fermat getallen uit de reeks voorkomen zijn we klaar. Dit kunnen we laten zien door aan te tonen dat het product van alle Fermat getallen kleiner dan F_n gelijk is aan $F_n - 2$ (voor $n \geq 1$). In het vervolg zullen we $\prod_{k=0}^{m} F_k$ gebruiken voor het product $F_0 \times F_1 \times \cdots \times F_m$. We gaan dus aantonen dat $\prod_{k=0}^{n-1} F_k = F_n - 2$ (voor $n \geq 1$).

Immers, als we deze betrekking kunnen aantonen, dan zien we: als q een deler is van F_k en van F_n, voor zekere $k < n$, dan moet q ook een deler zijn van 2. Dus $q = 1$ of 2. Maar $q = 2$ is onmogelijk, want alle Fermat getallen zijn oneven. De betrekking

$$\prod_{k=0}^{n-1} F_k = F_n - 2 \quad (n \geq 1)$$

wordt bewezen met inductie naar n. Voor $n = 1$ hebben we $F_0 = 3, F_1 = 5$ en $F_1 - 2 = 3$, dus dit klopt. De inductiestap gaat als volgt:

$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k\right) F_n \stackrel{ih}{=} (F_n - 2)F_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2.$$

Hiermee is het bewijs rond. ∎

2.6 Het GGD-algoritme van Euclides

In deze paragraaf laten we een voorbeeld zien waar een bewijs nauw samenhangt met een rekenmethode. Euclides heeft het oudste 'programma' of 'algoritme' op zijn naam, een programma om de grootste gemene deler (GGD) van twee positieve natuurlijke getallen a en b te vinden. De grootste gemene deler van a en b is het getal d met de volgende eigenschappen:

1. d deelt zowel a als b. (d is een gemeenschappelijke deler.)

2. voor geen getal k groter dan d geldt dat k zowel a als b deelt. (Er is geen grotere gemeenschappelijke deler dan d.)

Hier is Euclides' beroemde voorschrift om de GGD van twee positieve natuurlijke getallen a en b te berekenen.

ZOLANG $a \neq b$ DOE
ALS $a > b$ DAN $a := a - b$ ANDERS $b := b - a$.

In dit voorschrift worden a en b beschouwd als variabelen in een programmeertaal. Hier moet $a := a - b$ dus worden gelezen als: "maak de *nieuwe* waarde van a gelijk aan het verschil van de oude waarde van a en de oude waarde van b."

Om te zien hoe dit werkt kijken we naar een voorbeeld met $a = 30$ en $b = 84$. Neem aan dat het variabelen-paar (a, b) successievelijk de waarden (a_0, b_0), (a_1, b_1), (a_2, b_2) ... aanneemt. We krijgen dan:

	$a_0 = 30$	$b_0 = 84$
$a_0 < b_0$	$a_1 = 30$	$b_1 = 84 - 30 = 54$
$a_1 < b_1$	$a_2 = 30$	$b_2 = 54 - 30 = 24$
$a_2 > b_2$	$a_3 = 30 - 24 = 6$	$b_3 = 24$
$a_3 < b_3$	$a_4 = 6$	$b_4 = 24 - 6 = 18$
$a_4 < b_4$	$a_5 = 6$	$b_5 = 18 - 6 = 12$
$a_5 < b_5$	$a_6 = 6$	$b_6 = 12 - 6 = 6$
$a_6 = b_6 = 6$		

Inderdaad, 6 is de grootste gemene deler van 30 en 84, want 6 deelt beide getallen, en er is geen groter getal dan 6 dat beide getallen deelt.

Opdracht 2.11 *Voer zelf dit algoritme uit voor het getallenpaar $a = 90$, $b = 42$, en voor het getallenpaar $a = 90$, $b = 43$.*

Maar *waarom* geeft het algoritme de grootste gemene deler van a en b?

Stelling 2.1 *Als $a > b$ dan is d deler van a en b dan en slechts dan als d deler van $a - b$ en b is. Als $a < b$ dan is d deler van a en b dan en slechts dan als d deler van a en $b - a$ is.*

Opdracht 2.12 *Bewijs Stelling 2.1.*

Waarom volgt hier nu uit dat Euclides' algoritme inderdaad de grootste gemene deler uitrekent? Wat Stelling 2.1 zegt is dat elke lus door het algoritme de verzameling delers hetzelfde laat, in de volgende zin: de delers van a_i en b_i zijn hetzelfde als de delers van a_{i+1} en b_{i+1}.

Maar dan behoudt elke lus door het algoritme ook de grootste gemene deler van a en b. Omdat de getallen bij elke lus kleiner worden weten we ook dat het algoritme na het doorlopen van een eindig aantal lussen moet stoppen. Het algoritme stopt met $a_k = b_k$. Omdat a_k zeker de grootste gemene deler is van a_k en b_k, is a_k dus ook de grootste gemene deler van a_0 en b_0, dat wil zeggen van a en b.

Het GGD algoritme van Euclides kan worden gebruikt om een belangrijke eigenschap van grootste gemene delers te bewijzen. De GGD van 30 en 84 is 6, en we hebben dat $3 \cdot 30 - 84 = 6$. De GGD van 24 en 36 is 12, en we hebben dat $2 \cdot 24 - 36 = 12$. De GGD van 18 en 24 is 6, en we hebben dat $24 - 18 = 6$. De GGD van 3 en 5 is 1, en we hebben dat $-3 \cdot 3 + 2 \cdot 5 = 1$. In het algemeen geldt:

Stelling 2.2 *Als a en b positieve natuurlijke getallen zijn dan zijn er gehele getallen m en n met $ma + nb = GGD(a, b)$.*

Bewijs. Beschouw de paren $(a_0, b_0), (a_1, b_1), \ldots, (a_k, b_k)$ die worden gegenereerd door het algoritme van Euclides. We weten dat $a_0 = a$ en $b_0 = b$, en dat $a_k = b_k = \mathrm{GGD}(a, b)$.

a_0 voldoet aan $a_0 = ma + nb$ voor $m = 1, n = 0$, en b_0 voldoet aan $b_0 = ma + nb$ voor $m = 0, n = 1$.

Neem aan dat a_i voldoet aan $a_i = m_1 a + n_1 b$ en b_i voldoet aan $b_i = m_2 a + n_2 b$. Als $a_i > b_i$, dan voldoet a_{i+1} aan $a_{i+1} = (m_1 - m_2)a + (n_1 - n_2)b$ en b_{i+1} aan $b_{i+1} = m_2 a + n_2 b$. Als $a_i < b_i$, dan voldoet a_{i+1} aan $a_{i+1} = m_1 a + n_1 b$ en b_{i+1} aan $b_{i+1} = (m_2 - m_1)a + (n_2 - n_1)b$. Dus elke lus door Euclides' algoritme behoudt het feit dat a_i and b_i van de vorm $ma + nb$ zijn, voor geschikte m, n.

Dit laat zien dat er gehele getallen m, n zijn met $a_k = ma + nb$, en dus dat $ma + nb = \mathrm{GGD}(a, b)$. ∎

Dit resultaat stelt ons in staat om een belangrijke eigenschap van priemdelers te bewijzen.

Stelling 2.3 *Als p een priemgetal is dat ab deelt, dan moet p minstens een van de getallen a en b delen.*

Bewijs. Stel dat p deler is van ab, maar niet van a. Dan geldt dus dat $\mathrm{GGD}(a, p) = 1$, want p heeft immers alleen p en 1 als delers.

Uit de vorige stelling volgt dat er gehele getallen m, n zijn met:

$$ma + np = 1.$$

Vermenigvuldig nu aan beide zijden met b:

$$mab + nbp = b.$$

Uit het feit dat p deler is van ab weten we dat p zowel mab als nbp deelt. Dus p is deler van $mab + nbp$. Maar dan is p ook deler van b. ∎

Hiermee kunnen we vervolgens de zogenaamde *fundamentele stelling van de rekenkunde* bewijzen. Die stelling zegt dat elk geheel getal groter dan 1 een unieke ontbinding in priemfactoren heeft (uniek, afgezien van de volgorde van de factoren).

Stelling 2.4 (Fundamentele Stelling van de Rekenkunde) *Elk natuurlijk getal groter dan 1 heeft een unieke priem factorisering.*

Bewijs. Hier is een manier om een willekeurig natuurlijk getal n groter dan 1 in priemfactoren te ontbinden:

$$\text{ZOLANG } n \neq 1 \text{ DOE } (p := \text{KD}(n); n := \frac{n}{p}).$$

We weten (opdracht 2.3) dat KD(n) een priemgetal is, dus elke keer dat de lus wordt doorlopen wordt er een priemfactor p_i van het oorspronkelijke getal afgesplitst. Bij elke gang door de lus wordt n kleiner, dus deze procedure stopt na eindig veel stappen.

Dit laat zien dat elk natuurlijk getal groter dan 1 een priemfactorisering heeft. Wat we nu nog moeten laten zien is dat die priemfactorisering uniek is.

Neem aan dat er een getal N bestaat met minstens twee verschillende priemfactoriseringen. Dan zou voor N het volgende moeten gelden:

$$N = p_1 \cdots p_r = q_1 \cdots q_s,$$

met alle $p_1, \ldots, p_r, q_1, \ldots, q_s$ priem. Dus moet er een p_i zijn die niet voorkomt tussen de q's. Maar dat is in tegenspraak met Stelling 2.3, omdat p_i deler is van $N = q_1 \cdots q_s$ terwijl p_i geen van $q_1, \ldots, q_s$ deelt. Dit zijn immers allemaal priemgetallen die stuk voor stuk verschillend zijn van p_i. ∎

Met behulp van de fundamentele stelling van de rekenkunde kunnen we de irrationaliteit van $\sqrt{2}$ op nog een andere manier bewijzen.

Bewijs 4 van '$\sqrt{2}$ is geen breuk'. Als $\sqrt{2} = p/q$, dan is $2q^2 = p^2$. In de representatie van p^2 als product van priemfactoren zal elke priemfactor een even aantal malen voorkomen. Immers, het kwadraat van een getal is gelijk aan het product van de kwadraten van de priemfactoren van dat getal. In de representatie van $2q^2$ komt de factor 2 echter een oneven aantal malen voor. Omdat volgens Stelling 2.4 de representatie als product van priemfactoren uniek is (afgezien van de volgorde van de factoren) is dit onmogelijk. ∎

2.7 Opdrachten over bewijsmethoden

De volgende opdrachten geven je de kans generalisaties van en variaties op de stellingen uit Hoofdstuk 1 te onderzoeken. We beginnen met variaties op en generalisaties van Stelling 1.1.

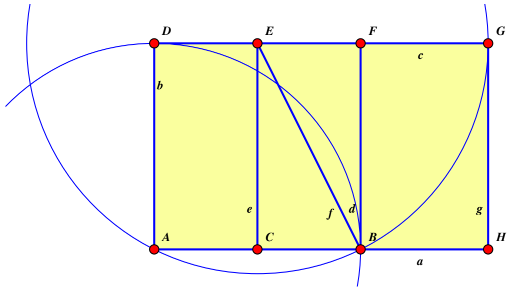
Opdracht 2.13 *Gebruik de methode van het bewijs van stelling 1.1 om te laten zien dat de wortel uit 3 geen breuk is.*

Opdracht 2.14 *Kun je nu ook laten zien dat $\sqrt{2} + \sqrt{3}$ geen breuk is?*

Opdracht 2.15 *Laat zien: als p priem is, dan is $\sqrt{p}$ geen breuk.*

Opdracht 2.16 *Laat zien: als n een natuurlijk getal is met de eigenschap dat $\sqrt{n}$ geen natuurlijk getal is, dan is $\sqrt{n}$ geen breuk.*

Opdracht 2.17 *Je herinnert je hopelijk nog de definitie van "de logaritme van a op basis b." Die definitie luidde: $L = {}^b\log a$ is de macht waartoe we basis b moeten verheffen om a te krijgen, dat wil zeggen, $b^L = a$. ${}^{10}\log 2$ is dus de macht (of exponent) waartoe we 10 moeten verheffen om 2 te krijgen. Kun je laten zien dat ${}^{10}\log 2$ geen breuk is?*

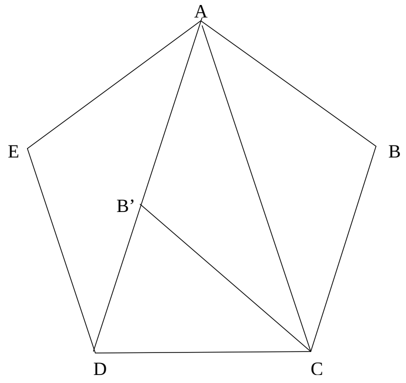


Figuur 2.2: De Gulden Snede.

Minstens even beroemd als de verhouding tussen de schuine zijde en de rechthoekzijde in een gelijkbenige rechthoekige driehoek is de verhouding tussen de lange zijde en de korte zijde in de rechthoek uit Figuur 2.2. Deze rechthoek heeft een bijzondere eigenschap: als je het vierkant $ABFD$ uit de rechthoek $AHGD$ verwijdert krijg je een nieuw rechthoek $HGFB$ met precies dezelfde verhouding tussen hoogte en breedte als in de oorspronkelijke rechthoek, met als enige verschil dat de nieuwe rechthoek op zijn kant staat. In de oudheid werd de verhouding tussen de lange zijde en de korte zijde in het rechthoek uit Figuur 2.2 gezien als de esthetisch ideale verhouding. Men noemde die verhouding de *gulden snede*. De waarde is bij benadering 1,61803.

Opdracht 2.18 *Laat zien dat de lange zijde en korte zijde van de rechthoek uit Figuur 2.2 zich verhouden als $\frac{1+\sqrt{5}}{2}$. Hoe kun je inzien dat deze verhouding geen breuk is?*

Opdracht 2.19 *Een regelmatige vijfhoek is een vijfhoek met vijf gelijke zijden en vijf gelijke hoeken. Laat zien dat de verhouding tussen de diagonaal en de zijde in een regelmatige vijfhoek*

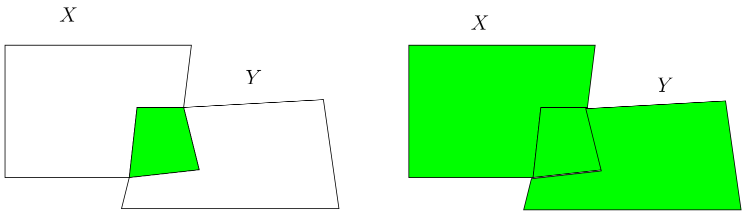


Figuur 2.3: Regelmatige vijfhoek.

gelijk is aan de gulden snede, dat wil zeggen aan $\frac{1+\sqrt{5}}{2}$. *Hint: zie de ingetekende driehoeken in Figuur 2.3.*

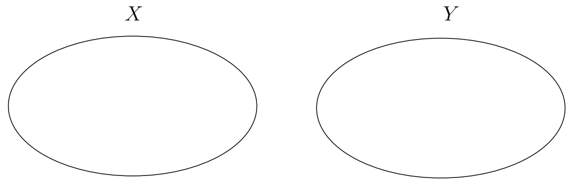
Opdracht 2.20 *Gebruik het stramien van het vierde bewijs van '$\sqrt{2}$ is geen breuk' (bladzijde 31) om te laten zien dat $\sqrt[3]{2}$ geen breuk is.*

Voordat we afsluiten met een variant op Stelling 1.2 eerst een beetje verzamelingenleer. Figuur 2.4 maakt aanschouwelijk wat we bedoelen met de doorsnede $X \cap Y$ en de vereniging $X \cup Y$ van twee verzamelingen X en Y. $X \cap Y$ is de verzameling van elementen die zowel in X als in Y zitten, $X \cup Y$ de verzameling van elementen die in minstens één van X, Y zitten.



Figuur 2.4: Twee verzamelingen X en Y met links hun doorsnede $X \cap Y$, rechts hun vereniging $X \cup Y$ gekleurd.

We gebruiken $\emptyset$ voor de verzameling met niets erin. We noemen dit de *lege* verzameling. Dus in Figuur 2.5 geldt dat $X \cap Y = \emptyset$. We zeggen dan dat X en Y disjunct zijn.



Figuur 2.5: Twee disjuncte verzamelingen X en Y: de verzameling $X \cap Y$ is leeg.

Om te zeggen dat n een natuurlijk getal is gebruiken we de afkorting: $n \in \mathbb{N}$. Dit staat voor: 'n is een element van de verzameling van natuurlijke getallen'. Hierbij staat '$\in$' voor 'is een element van'. De even natuurlijke getallen zijn alle natuurlijke getallen van de vorm $2n$. Om de verzameling even natuurlijke getallen aan te duiden gebruiken we de volgende accolade-notatie:

$$\{2n \mid n \in \mathbb{N}\}.$$

Net zo kunnen we de verzameling aanduiden van natuurlijke getallen die bij deling door 4 rest 3 geven:

$$\{4n + 3 \mid n \in \mathbb{N}\}.$$

In de volgende opdracht moet je laten zien dat de doorsnede van deze laatste verzameling met de verzameling priemgetallen oneindig is. Met andere woorden: er zijn oneindig veel priemgetallen die rest 3 geven als je ze door 4 deelt.

Opdracht 2.21 *Behalve 2 zijn alle priemgetallen oneven. Als je zo'n oneven priemgetal door 2 deelt krijg je dus altijd rest 1. Als je zo'n oneven priemgetal door 4 deelt krijg je ofwel een rest 1 of een rest 3. Als je geen rest of een rest 2 zou krijgen zou het getal immers even zijn.*

De getallen die wanneer je ze door 4 deelt rest 1 geven zijn van de vorm $4n + 1$, voor een of ander natuurlijk getal n. De getallen die wanneer je ze door 4 deelt rest 3 geven zijn van de vorm $4n + 3$.

Laat zien dat er oneindig veel priemgetallen zijn die wanneer je ze door 4 deelt rest 3 geven. Met andere woorden, laat A de verzameling $\{4n+3 \mid n \in \mathbb{N}\}$ zijn, en laat B de verzameling zijn van alle priemgetallen. Laat zien dat $A \cap B$ oneindig is.

Hier is een aanwijzing. *Begin met aan te nemen dat er maar eindig veel priemgetallen van de vorm $4n+3$ zijn, zeg, $p_1, \ldots, p_m$. Beschouw nu het getal $Q = 4p_1 \cdots p_m - 1 = 4(p_1 \cdots p_m - 1) + 3$. Laat zien dat Q een factor $4q + 3$ moet hebben. Daarvoor kun je gebruik maken van het feit dat $(4a + 1)(4b + 1)$ van de vorm $4c + 1$ is.*

2.8 Een fout bewijs is geen bewijs

Bij het vertrouwen op inzicht moet je wel voorzichtig zijn. Je kunt denken dat je iets ziet, maar je toch vergissen. Wie zich hierover zorgen maakt heeft behoefte aan een bewijs.

Hier is een beroemd raadsel van de eerwaarde heer Charles Lutwidge Dodgson, beter bekend als Lewis Carroll, de man die *Alice in Wonderland* schreef. In een ondoorzichtige zak zit een papiertje, waarvan we alleen weten dat het wit of zwart is. Nu maakt iemand de zak open en stopt er een wit papiertje bij, waarna de zak met de twee papiertjes flink wordt geschud. Vervolgens halen we, zonder te kijken, een papiertje uit de zak. Het blijkt wit te zijn. Hoe groot is nu de waarschijnlijkheid dat het papiertje dat nog in de zak zit ook wit is?

Nu zou je als volgt kunnen redeneren. Voordat het extra witte papiertje in de zak wordt gestopt is de waarschijnlijkheid dat het ene papiertje in de zak wit is $\frac{1}{2}$. Nu wordt er vervolgens een wit papiertje bij gestopt en een wit papiertje uit gehaald. Daarmee zijn we terug bij de oude situatie, en is de waarschijnlijkheid dat het overgebleven papiertje in de zak wit is dus weer $\frac{1}{2}$. Deze redenering oogt misschien plausibel, maar zij is *fout*.

Opdracht 2.22 *Doe nu zelf: hoe groot is de waarschijnlijkheid dat het papiertje dat nog in de zak zit ook wit is? (Hint: het antwoord $\frac{1}{2}$ is dus fout.)*

Als je hier uit komt zul je zeker ook het volgende probleem kunnen oplossen. Het hele eieren eten is het vinden van de juiste manier om de zaak te bekijken.

Opdracht 2.23 *In een gezin zijn twee kinderen. Minstens één daarvan is een jongen. Hoe groot is de waarschijnlijkheid dat beide kinderen jongens zijn? In een ander gezin, ook met twee kinderen, is het oudste kind een meisje. Hoe groot is de waarschijnlijkheid dat beide kinderen meisjes zijn?*

Hier is nog een voorbeeld waarbij het gemakkelijk is de fout in te gaan met redeneren. Stel, je bent de laatst overgebleven kandidaat in een TV quiz, en je slotopdracht is te kiezen tussen drie deuren 1, 2 en 3. Achter een van de deuren staat de hoofdprijs van de quiz (een fonkelnieuwe cabrio), achter de twee andere deuren zit niets. Je kiest deur 1. De quizmaster speelt nog even een spelletje met je, en probeert je aan het twijfelen brengen. Hij doet deur 2 open en laat zien dat de cabrio *niet* achter die deur staat. Hij vraagt "Blijf je bij je keus van deur 1? Of wil je toch liever deur 3?" Je redeneert nu als volgt: er zijn nog twee deuren over, en de cabrio kan achter allebei zitten. Het maakt dus niet uit welke van die twee deuren ik kies. Er is geen reden om mijn keuze te herzien. Deze redenering oogt misschien plausibel, maar zij is *onjuist*.

Opdracht 2.24 *Wat is je kans om de cabrio te winnen als je bij je eerste keus blijft? Wat is je kans om te winnen als je je keuze herziet?*

Hier zijn nog een paar beroemde voorbeelden van mathematische drogredenen. We gaan bewijzen dat $1 = 2$. Dat gaat als volgt.

1. Voor elke a geldt dat $a(a-a) = a^2 - a^2$.

2. Maar het volgende geldt ook: $a^2 - a^2 = (a+a)(a-a)$.
3. Uit $a(a-a) = (a+a)(a-a)$ volgt dat $a = a + a$.
4. Maar dan is $a = 2a$.
5. Delen van beide kanten door a geeft $1 = 2$. QED.

Net zo kun je bewijzen dat $2 = 1$. Dat doen we als volgt.

1. Stel dat $a = b$. Dan volgt hieruit zeker dat $a^2 = ab$.
2. Links en rechts b^2 aftrekken geeft $a^2 - b^2 = ab - b^2$.
3. Ontbinden geeft: $(a+b)(a-b) = b(a-b)$.
4. Dit kunnen we vereenvoudigen met delen door $a - b$. Dit geeft $a + b = b$.
5. Omdat a en b aan elkaar gelijk zijn volgt hieruit $2b = b$.
6. Maar dan geeft delen door b dat $2 = 1$. QED.

Opdracht 2.25 *Waar zit de fout in bovenstaande redeneringen?*

Nog een voorbeeld. We bewijzen nu dat $0 = 1$. Neem de volgende oneindige reeks.

$$1 - 1 + 1 - 1 + 1 - 1 + 1 - 1 + \cdots$$

De som van deze reeks is 0 als je de haakjes zo zet:

$$(1-1) + (1-1) + (1-1) + (1-1) + \cdots$$

De som van de reeks is 1 als je de haakjes zo zet:

$$1 + (-1+1) + (-1+1) + (-1+1) + \cdots$$

Dus $0 = 1$. QED.

Opdracht 2.26 *Waar zit de fout in deze redenering?*

Tenslotte een voorbeeld van een merkwaardig "bewijs" met behulp van inductie. We "bewijzen" met volledige inductie dat voor elke eindige verzameling A en voor elke eigenschap E geldt dat ofwel alle elementen van A eigenschap E hebben ofwel geen van de elementen van A heeft eigenschap E. Dit impliceert bij voorbeeld dat de inwoners van Amsterdam of allemaal mannen zijn of allemaal vrouwen. We "bewijzen" dit met inductie naar de grootte van de verzameling A.

Basisstap Neem aan dat de verzameling A slechts 1 element bevat. Als dat element eigenschap E heeft dan hebben alle elementen van A de eigenschap, anders heeft geen element van A de eigenschap. Dus: ofwel alle elementen van A zijn E, ofwel geen element van A is E.

Inductiestap Neem aan dat elke verzameling van n elementen ofwel bestaat uit alleen Es, ofwel bestaat uit alleen niet-Es. Dit is onze inductiehypothese. We laten zien dat dit ook geldt voor verzamelingen met $n+1$ elementen. Neem dus aan dat A een verzameling is van $n+1$ elementen. Nu selecteren we willekeurig twee individuen p en q uit A. We laten zien dat die twee ofwel allebei E hebben, ofwel allebei niet-E.

Merk op dat $A-\{p\}$ (de verzameling die je krijgt door element p uit A te halen) en $A-\{q\}$ (de verzameling die je krijgt door element q uit A te halen) allebei n elementen hebben, dus de inductiehypothese geldt voor deze verzamelingen. Neem nu $r \in A - \{p, q\}$. Dat moeten r en p ofwel allebei E hebben ofwel geen van beide. Net zo voor r en q. Maar dan hebben p en q ofwel allebei E ofwel geen van beide. In het eerste geval hebben alle elementen van A eigenschap E, in het het tweede heeft geen element van A de eigenschap. QED.

Opdracht 2.27 *Waar zit de fout in deze redenering?*

Hoofdstuk 3

Geschiedenis van de Axiomatische Methode

3.1 Aristoteles over de axiomatische methode

Aristoteles (een Griekse filosoof uit de vijfde eeuw voor Christus) identificeerde de volgende twee basisingrediënten van abstract redeneren: *begrippen* en *beweringen*. Begrippen dienen om de zaken te omschrijven waarop het redeneren betrekking heeft. Zij maken het redeneren mogelijk. Beweringen zijn de uitspraken die je doet over zaken die je met behulp van begrippen hebt gedefinieerd. Begrippen dienen te worden *gedefinieerd* en beweringen dienen te worden *bewezen*.

Een *definitie* is een omschrijving van de betekenis van een begrip in termen van andere begrippen. Aristoteles merkte op dat het niet mogelijk is om van elk begrip een definitie te geven. Het proces van definiëren kan immers niet eindeloos terug gaan. Sommige begrippen zijn *primitieve begrippen*. Je wordt geacht onmiddellijk te 'zien' wat ze betekenen. Een voorbeeld uit de meetkunde is het begrip 'punt'. Euclides doet wel een (zwakke) poging om een punt te omschrijven als 'dat wat geen delen heeft', maar die definitie wordt verder nooit gebruikt, en ook wordt niet uitgelegd wat het betekent om een deel te zijn van iets. Een voorbeeld van een primitief begrip uit de moderne wiskunde is het begrip 'verzameling'.

Opdracht 3.1 *Zoek het woord* verzameling *op in een woordenboek van het Nederlands, bij voorbeeld* Van Dale. *Zoek vervolgens de woorden op die gebruikt worden in de omschrijving, dan de woorden die gebruikt worden in de omschrijvingen van die woorden, enzovoort. Waar stopt dit proces?*

Net zo min als elk begrip een definitie heeft, heeft elke bewering een bewijs. Bewijzen van een bewering A doe je door A met behulp van een *bewijsregel* af te leiden uit andere beweringen, zeg B en C:

$$\frac{B \quad C}{A}$$

Bewijzen van B doe je door B met behulp van een bewijsregel af te leiden uit weer andere bewerkingen, bij voorbeeld D en E.

$$\frac{\dfrac{D \quad E}{B} \quad C}{A}$$

Net zo voor bewijzen van C. Bewijzen van D doe je door D met behulp van een bewijsregel af te leiden uit nog weer andere beweringen, enzovoort.

Stel nu dat je elke bewering zou moeten bewijzen door afleiding uit andere beweringen. Het bewijs van A zou dan oneindig lang worden. Er moeten dus beweringen zijn die geen bewijs nodig hebben of die niet bewezen kunnen worden. Zulke beweringen heten *axioma's*. Een onderwerp kan worden uitgediept door, beginnende bij axioma's en basisbegrippen, nieuwe begrippen te definiëren, en nieuwe beweringen te bewijzen uit axioma's en eerder bewezen beweringen. Zo'n bewezen bewering heet een *stelling*. Aristoteles was de eerste die een poging waagde om de manier waarop het bewijsproces werkte expliciet te maken. Zijn theorie over syllogismen was de eerste poging om het redeneren te formaliseren. Hier is een voorbeeld van zo'n syllogisme:

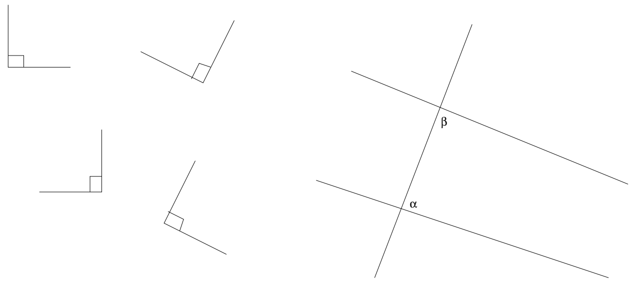
$$\frac{\text{Alle Grieken zijn mensen.} \quad \text{Alle mensen zijn sterfelijk.}}{\text{Alle Grieken zijn sterfelijk.}}$$

3.2 Euclides' axiomatische presentatie van de meetkunde

Het beroemdste voorbeeld aller tijden van het gebruik van de axiomatische methode is de systematische presentatie van de meetkunde in de *Elementen* van Euclides [9]. Euclides vatte hierin samen wat de Griekse wiskundigen in zijn tijd van meetkunde wisten.

Euclides presenteerde de meetkunde-kennis van zijn tijd in streng axiomatische vorm. Axioma's had Euclides in twee soorten: axioma's die niets met meetkunde van doen hebben (bij voorbeeld: 'als je gelijke grootheden bij gelijke grootheden optelt krijg je gelijke uitkomsten', dat wil zeggen: 'als $a = 2$ en $b = 3$ dan $a + b = 2 + 3$') en meetkundige axioma's. De axioma's van meetkundige aard noemde hij *postulaten*. Dit zijn de vijf postulaten die Euclides aanneemt (illustraties van postulaten IV en V zijn te vinden in Figuur 3.1):

- I Een tweetal punten kan door precies één lijnstuk met elkaar worden verbonden.
- II Een lijnstuk kan worden doorgetrokken in precies één lijn.
- III Een punt P en een lengte r bepalen een cirkel met middelpunt P en straal r.
- IV Alle rechte hoeken zijn congruent (gelijk).
- V Als een lijn twee lijnen snijdt, met de twee binnenhoeken aan dezelfde zijde samen kleiner dan twee rechte hoeken, dan zullen de twee lijnen elkaar aan die zijde snijden.



Figuur 3.1: Illustraties van postulaten IV en V.

De postulaten zijn geformuleerd in termen van begrippen zoals 'punt', 'lijnstuk', 'lijn', 'cirkel', 'snijden', 'doortrekken', enzovoorts. Wat is de status van die begrippen? Het is de vraag of Euclides beseft heeft dat in een axiomatisch systeem primitieve begrippen niet te vermijden zijn. Hij doet tenminste zijn best om *alle* begrippen te definiëren. Sommige van die omschrijvingen zijn bruikbaar en heel precies, maar andere lijken alleen bedoeld om het voorstellingsvermogen van de lezer een handje te helpen.

Nu doet zich het verrassende feit voor dat er uit deze postulaten allerlei beweringen ("stellingen") volgen waarvan je op het eerste gezicht helemaal niet zou zeggen dat ze in de postulaten besloten liggen.

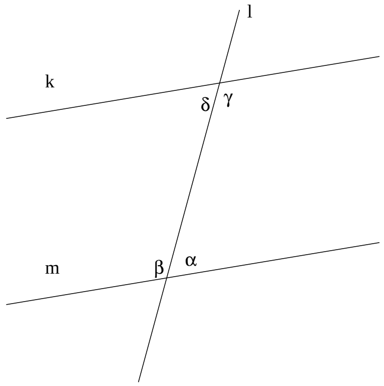
Als voorbeeld van hoe je de postulaten kunt gebruiken om de waarheid van verrassende beweringen aan te tonen geven we het bewijs van het welbekende feit dat som van de drie hoeken van een driehoek gelijk is aan 180° (dat wil zeggen, aan twee rechte hoeken). Allereerst laten we zien dat als een lijn l twee parallelle lijnen m en k snijdt, de twee overstaande hoeken (dat wil zeggen: verwisselde binnenhoeken) gelijk zijn (Figuur 3.2).

Uit het feit dat de lijnen m en k elkaar niet snijden aan de zijde van de hoeken α en γ kunnen we concluderen, met behulp van postulaat V, dat $\alpha + \gamma$ *niet* kleiner is dan twee rechte hoeken. Anders gezegd, $\alpha + \gamma \geq 180°$. Merk nu op dat γ en δ samen een gestrekte hoek vormen, dat wil zeggen $\gamma + \delta = 180°$. Samen met $\alpha + \gamma \geq 180°$ geeft dit $\alpha + (180° - \delta) \geq 180°$. Hieruit volgt $\alpha \geq \delta$. Net zo volgt uit het feit dat m en k elkaar niet snijden aan de zijde van de hoeken β en δ dat $\delta + (180° - \alpha) \geq 180°$, dus $\delta \geq \alpha$. Samen met $\alpha \geq \delta$ geeft dit $\alpha = \delta$.

Uit $\alpha = \delta$ volgt $180° - \alpha = 180° - \delta$, dat wil zeggen: $\beta = \gamma$. Hiermee is het gevraagde bewezen.

Je kunt uit postulaten I t/m IV de volgende stelling bewijzen. Stel je hebt een lijn en een punt niet op die lijn. Dan gaat er door dat punt een lijn die evenwijdig is met de gegeven lijn (Figuur 3.3. We zullen nu gebruik maken van deze stelling zonder hem te bewijzen.

Nu we dit eenmaal hebben is het bewijs dat de som van de drie hoeken van een driehoek gelijk is aan 180° niet moeilijk meer. Zie de driehoek in Figuur 3.4, met een lijn door de



Figuur 3.2: Een gevolg van postulaat V: $\alpha = \delta$ en $\beta = \gamma$.

tophoek van de driehoek parallel aan de basis. Dat zo'n lijn er moet zijn volgt uit de zojuist genoemde stelling. Uit wat we daarvoor hebben bewezen weten we dat $\alpha = \delta$ en $\beta = \epsilon$, dus $\alpha + \beta + \gamma = \delta + \gamma + \epsilon = 180°$, en dat is precies wat bewezen moest worden.

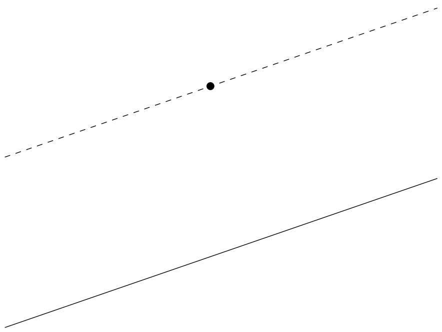
Opdracht 3.2 *Laat nu zelf zien dat als twee lijnen m en n elkaar snijden, de overstaande hoeken congruent (gelijk) zijn. Welk postulaat heb je hiervoor nodig?*

Euclides laat af en toe kleine steekjes vallen door hier en daar begrippen te hanteren waar extra axioma's voor nodig zijn die echter niet worden gegeven. Als drie punten A, B en C op een lijn liggen, dan moet een van die punten tussen de twee andere liggen. Dan zijn er immers drie mogelijkheden: A ligt op het lijnstuk BC, B ligt op het lijnstuk AC, of C ligt op het lijnstuk AB. Hoe je dit begrip 'liggen tussen' moet gebruiken wordt echter niet uitgelegd. Nu zou je kunnen denken dat iedereen zonder uitleg toch wel weet wat 'liggen tussen' betekent. Maar dat is hier niet genoeg, want voor *echt* weten wat 'liggen tussen' betekent in de zin waar het hier om draait zijn twee dingen nodig:

1. weten hoe je het gegeven dat x tussen y en z ligt mag *gebruiken* in een bewijs van iets anders, en

2. weten wat je moet doen om de bewering "x ligt tussen y en z" te *bewijzen*.

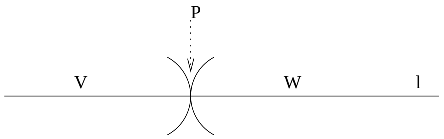
Bij Euclides speelt de aanschouwing wel degelijk nog een rol. Dat blijkt al uit zijn allereerste stelling, die luidt: voor elk gegeven lijnstuk bestaat er een gelijkzijdige driehoek met dat lijnstuk als een van de zijden. Euclides geeft dan de bekende constructie die je ziet in Figuur 3.5.



Figuur 3.3: Evenwijdige lijn door een punt buiten een lijn.

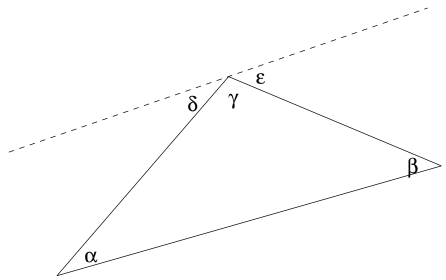
Laat AB het gegeven lijnstuk zijn. Trek een cirkel met middelpunt A die door B gaat. Trek vervolgens een cirkel met middelpunt B die door A gaat. Noem een van de punten waar de cirkels elkaar snijden C, en voila, $\triangle ABC$ is een gelijkzijdige driehoek. Maar het merkwaardige feit doet zich voor dat je uit de postulaten van Euclides niet kunt afleiden dat de twee cirkels elkaar in een punt C zullen snijden. Daarvoor is een extra axioma nodig dat pas in de Negentiende eeuw voor het eerst werd geformuleerd door Dedekind (1831–1916), het zogenaamde continuïteitsaxioma:

> Laat de verzameling van alle punten op een lijn l de vereniging zijn van twee puntverzamelingen V en W, met de eigenschap dat geen punt uit V tussen twee punten uit W ligt en andersom. Dan is er een uniek punt P op l met de eigenschap dat P op het lijnstuk QR ligt precies dan wanneer $Q \in V$ en $R \in W$.



Dit lijkt misschien een vanzelfsprekendheid, maar dat is het niet. Als je punten in een vlak voorstelt als paren van breuken $(\frac{p}{q}, \frac{r}{s})$, waarbij $\frac{p}{q}$ de x-coördinaat is $\frac{r}{s}$ de y-coördinaat, dan zou een rechte lijn eruit kunnen zien als een verzameling van zulke punten. Neem bij voorbeeld de verzameling $l = \{(3, q) \mid q \in \mathbb{Q}\}$, waarbij $\mathbb{Q}$ de verzameling is van alle breuken. Dit zou de vertikale lijn zijn door het punt met coördinaten $(3, 0)$. Maar we hebben gezien (Stelling 1.1) dat l het punt $(3, \sqrt{2})$ niet bevat. De moeilijkheid is dat l niet voldoet aan het continuïteitsaxioma, want l bestaat uit de vereniging van de verzamelingen

$$V = \{(3, q) \mid q \in \mathbb{Q}, q \leq 0 \text{ of } q^2 < 2\}$$



Figuur 3.4: De som van de hoeken van een driehoek is gelijk aan 180°.

en

$$W = \{(3, q) \mid q \in \mathbb{Q}, q > 0 \text{ en } q^2 > 2\}.$$

Maar, zoals we weten uit Stelling 1.1, het punt $(3, \sqrt{2})$ dat precies op de 'grens' tussen V en W ligt, zit niet in l.

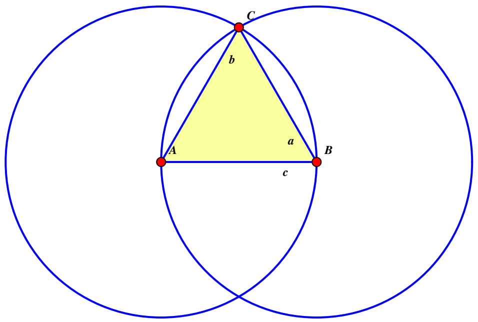
Met behulp van het continuïteitsaxioma kan worden bewezen dat als een cirkel zowel een punt binnen als een punt buiten een andere cirkel heeft, die twee cirkels elkaar in twee punten snijden.

Maar we zijn nu eigenlijk aan het zeuren over schoonheidsfoutjes. Ze doen niets af aan het feit dat de *Elementen* van Euclides beschouwd kan worden als het indrukwekkendste wetenschappelijke werk dat ons uit de klassieke Oudheid is nagelaten.

Het is niet helemaal duidelijk hoeveel eigen bijdragen van Euclides er in de *Elementen* verwerkt zitten. Zeer waarschijnlijk is het grootste deel ontleend aan voorgangers waarvan het werk voor ons verloren is gegaan. Maar de presentatie is van Euclides zelf. En die presentatie is reden genoeg om bewondering te hebben voor zijn diepe inzicht in zijn onderwerp. De keuze van zijn vijf meetkundige postulaten was zonder meer briljant. Vele wiskundigen hebben in de loop van de geschiedenis geprobeerd Euclides te verbeteren door te laten zien dat de vijf postulaten niet onafhankelijk van elkaar zijn. Ze dachten dan te kunnen laten zien dat je één van de postulaten uit de andere postulaten kunt afleiden.

Die pogingen concentreerden zich met name op het vijfde postulaat, dat er inderdaad anders uitziet dan de andere vier. Tal van pogingen zijn ondernomen om het vijfde postulaat uit de overige vier af te leiden, maar het is nooit iemand gelukt. Euclides had dus heel goed gezien dat dit postulaat niet kon worden gemist.

Nu was er wel enige reden om het vijfde postulaat te wantrouwen. De vier eerste postulaten zijn stuk voor stuk zeer eenvoudige beweringen, maar het vijfde postulaat oogt een stuk ingewikkelder. De ingewikkelder formulering suggereert dat het een stelling zou moeten zijn in plaats van een axioma. Alle pogingen om die stelling te bewijzen zijn echter mislukt, of ze bleken toch weer te berusten op een aanname die equivalent was aan het vijfde postulaat.



Figuur 3.5: Constructie van een gelijkzijdige driehoek.

Zo leidden de pogingen van de Griekse wiskundige Proclus (410–485) om het vijfde postulaat te bewijzen tot de volgende herformulering van het vijfde postulaat:

> Gegeven een lijn een punt buiten die lijn is het mogelijk om precies één lijn door het punt te trekken parallel aan de gegeven lijn.

Deze herformulering maakt duidelijk waarom Euclides' vijfde postulaat ook wel wordt aangeduid als het *parallellenpostulaat*.

Het blijkt echter dat, gegeven de andere axioma's, het parallellenpostulaat zoals gegeven door Euclides equivalent is met allerlei andere principes. Anders gezegd, er zijn heel verschillende principes X zodat X bewezen kan worden uit axioma's I tot en met V, maar zodat, andersom, axioma V volgt uit axioma I tot en met IV verrijkt met X. Hier heb je enige mogelijke X-en (ontleend aan [17], blz 128-129).

1. Parallelle rechte lijnen hebben overal dezelfde afstand van elkaar. (Poseidonius, 100 voor Christus)
2. Alle punten die op dezelfde afstand liggen van een gegeven rechte lijn, aan dezelfde kant, vormen samen een rechte lijn. (Clavius, 1574)
3. Er bestaan twee verschillende lijnen die overal gelijke afstand tot elkaar hebben.
4. De afstand tussen twee parallelle lijnen is overal kleiner dan een gegeven vaste afstand. (Proclus, 5e eeuw)
5. Rechte lijnen parallel met een gegeven rechte lijn, zijn parallel met elkaar.

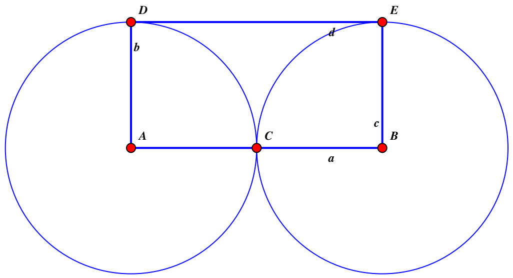
6. Door een gegeven punt niet op een gegeven lijn gaat hoogtens één lijn parallel aan de gegeven lijn. (Playfair, 18e eeuw)
7. Op een gegeven lijnstuk kunnen we altijd een driehoek construeren die gelijkvormig is met een gegeven driehoek. (Wallis 1663)
8. Er bestaat een paar niet congruente, gelijkvormige driehoeken. (Saccheri, 1733)
9. De som van de hoeken van een driehoek is 180°. (Saccheri, 1733)
10. Je hebt driehoeken met willekeurig groot oppervlak. (Gauss, 1799)
11. Door drie punten die niet op een lijn liggen gaat precies één cirkel. (Legendre, Bolyai, 19e eeuw)

Laten we eerst constateren dat sommige van deze axioma's wel duidelijk lijken, maar dat ze ook volkomen en direct inzichtelijk zijn, dat zou je toch niet zeggen. Er is nog een tweede punt. Waarom zouden we het ene axioma prefereren boven het andere? Je kunt allerlei redenen bedenken voor zo'n voorkeur. Eénvoud van formulering is één zo'n reden. Vergelijk bijvoorbeeld de oorspronkelijke versie van axioma V en principe (3). Principe (3) ziet er beduidend simpeler uit. Naast éénvoud van formulering hebben we een andere vorm van éénvoud: het aantal begrippen dat in een axioma gebruikt wordt. Axioma V en principe (3) maken naast de begrippen lijn, punt en *liggen op* gebruik van respectievelijk het begrip hoek en het begrip afstand. Het axioma van Playfair (principe (6)) maakt alleen gebruik van lijn, punt en *liggen op*. Het kan dus ook gebruikt worden in wiskundige theorieën die alleen over lijnen en punten en *liggen op* gaan. Een andere reden om de voorkeur te geven aan een axioma is makkelijke toepasbaarheid. Geen van bovenstaande principes voldoet aan die eis. In termen van directe inzichtelijkheid zijn er echter vele kandidaten die niet onder doen voor axioma V. Wat te denken van principe (8), dat ons vertelt dat de notie *vorm* überhaupt zin heeft? Of is er iets voor de hand liggender dan het principe van Gauss (10)? Het zou toch te gek zijn als je geen driehoeken kon maken met willekeurig groot oppervlak?

3.3 Saccheri's poging om het vijfde postulaat te bewijzen

De interessantste poging om het vijfde postulaat te bewijzen is van de Italiaanse priester Girolamo Saccheri (1667–1733). Hij ging te werk volgens de strategie van het 'bewijs door contradictie' (zie 5.5). Hij nam dus aan dat het vijfde postulaat *niet* gold, en zette zich aan het werk om een tegenspraak af te leiden. Zijn bedoeling was om alle fouten in Euclides' werk te herstellen (zijn boek uit 1733 heette *Euclides ab omni naevo vindicatus*, ofwel: *Euclides van elke smet gezuiverd*), en wel met name de 'fout' van de aanname van het vijfde postulaat.

Saccheri's bewijspoging van het vijfde postulaat maakt gebruik van de Saccheri vierhoek die staat afgebeeld in Figuur 3.6. Details zijn te vinden op de website bij dit boek, waar ook een interactieve pagina `Saccheri.html` te vinden is. Daar wordt aangetoond, zonder gebruik te maken van het vijfde postulaat, dat de twee tophoeken van de Saccheri vierhoek aan elkaar gelijk zijn. Er zijn nu precies drie mogelijkheden:



Figuur 3.6: De vierhoek van Saccheri.

1. De tophoeken zijn rechte hoeken.

2. De tophoeken zijn stompe hoeken (groter dan rechte hoeken).

3. De tophoeken zijn scherpe hoeken (kleiner dan rechte hoeken).

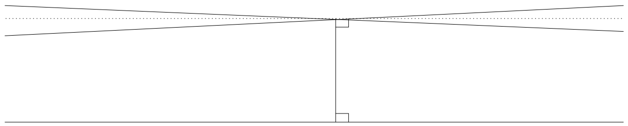
Saccheri liet zien dat als één van deze drie hypothesen opgaat voor een bepaalde Saccheri vierhoek, de hypothese moet gelden voor *elke* Saccheri vierhoek. Het kostte Saccheri niet veel moeite om aan te tonen dat uit de aanname dat de tophoeken recht zijn, het vijfde postulaat kan worden afgeleid. Ook lukte het hem uit de aanname dat de tophoeken stomp zijn, een contradictie af te leiden. Anders was het gesteld met de aanname dat de tophoeken scherp zijn.

Saccheri exploreerde de 'hypothese van de scherpe hoeken', in de hoop en verwachting op een tegenspraak te stuiten. Er gebeurde nu echter iets merkwaardigs. Saccheri leidde allerlei vreemde stellingen af, zoals:

- De som van de hoeken van een driehoek is kleiner dan twee rechte hoeken.

- Twee rechte lijnen in hetzelfde vlak hebben ofwel een gemeenschappelijke loodlijn, ofwel ze snijden elkaar op eindige afstand van een gegeven punt op een van de lijnen, ofwel ze komen steeds dichter bij elkaar zonder elkaar ooit te snijden.

- In een punt buiten een rechte lijn zijn altijd twee rechte lijnen aan te wijzen die de rechte lijnen die de eerste rechte lijn snijden afgrenzen van de rechte lijnen die dat niet doen. Onder de rechte lijnen die de eerste rechte lijn niet snijden is er een die een gemeenschappelijke loodlijn heeft met die eerste lijn (Figuur 3.7).



Figuur 3.7: Oneindig veel lijnen parallel aan een gegeven lijn.

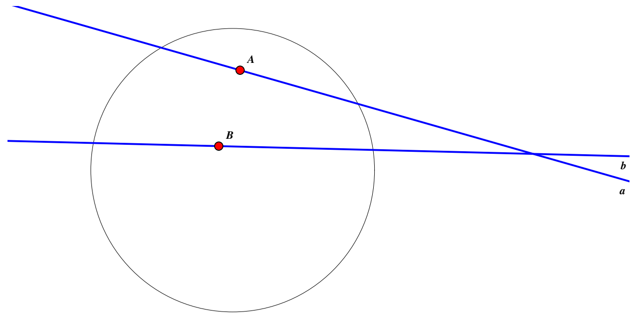
Saccheri had in feite een nieuwe wereld ontdekt, maar zonder het zelf te beseffen. Hij eindigt zijn boek met de conclusie dat de stellingen die hij afgeleid heeft aantonen dat "de hypothese van de scherpe hoek absoluut onjuist is, omdat hij strijdig is met de aard van de rechte lijn."

3.4 Niet-euclidische meetkunde

Saccheri's poging om een contradictie af te leiden uit het vijfde postulaat had een nieuwe wereld kunnen openen, maar om die nieuwe wereld te kunnen betreden moest je allereerst geloven dat die wereld ook kon bestaan. En daarvoor moest je grote filosofen zoals Immanuel Kant durven tegenspreken. De filosoof Plato had al eens gezegd dat de werkelijkheid meetkundig van aard is. Kant is specifieker. Volgens hem is het een waarheid als een koe (in Kants filosofisch jargon: "een synthetische waarheid a priori") dat wij leven in een Euclidische ruimte, een ruimte die voldoet aan de vijf postulaten van Euclides.

De eerste wiskundige die een duidelijk beeld heeft van een meetkunde die wezenlijk anders is dan die van Euclides is Karl Friedrich Gauss (1777–1855). Als twintiger begon Gauss na te denken over de theorie van parallellen. Hij zag snel in waar de diepe moeilijkheid vandaan kwam om het parallellenpostulaat uit de andere postulaten af te leiden, en hij begon met het ontwikkelen van een nieuwe meetkunde die hij *niet-euclidisch* noemde, maar zonder zijn resultaten openbaar te maken. Gauss had absoluut geen zin in heibel met de machtige aanhangers van Immanuel Kant. In een brief aan zijn vriend Taurinus uit 1824 stelt hij dat de aanname dat de som van de hoeken van een driehoek kleiner is dan 180° tot een merkwaardige meetkunde leidt, met stellingen die op het eerste gezicht paradoxaal en absurd lijken, maar "waarvan rustige overdenking leert dat ze niets onmogelijks bevatten." In diezelfde brief drukt hij zijn vriend op het hart om hier toch vooral geen ruchtbaarheid aan te geven.

In 1833 publiceerde een oude studiemakker van Gauss een meetkundige verhandeling in twee delen met een appendix van 26 bladzijden geschreven door zijn zoon, János Bolyai. In 1832 kreeg Gauss een proefdruk toegestuurd van de appendix. In die appendix werden de consequenties onderzocht van de veronderstelling dat er in een punt buiten een lijn ofwel geen ofwel meer dan één parallel bestaat aan een gegeven lijn. De eerste mogelijkheid wordt snel verworpen (net als Saccheri's stompe hoek hypothese). De tweede mogelijkheid leidt tot een interessante nieuwe meetkunde (de meetkunde corresponderend met Saccheri's scherpe hoek hypothese). Geheel anders dan Saccheri was János Bolyai ervan overtuigd dat hij een nieuw soort meetkunde aan het ontwikkelen was. Het antwoord van Gauss dat hij het allemaal al eerder gedaan had moet een zware slag zijn geweest voor de jonge Bolyai. Tot overmaat van ramp bleek later ook nog dat een onbekende Russische professor, Nikolai Lobachevski (1793–1856), de nieuwe meetkunde ook had ontdekt, en al in 1829 zijn resultaten had gepubliceerd.



Figuur 3.8: Parallelle lijnen in het Klein-Beltrami model.

3.5 Klein-Beltrami modellen voor niet-euclidische meetkunde

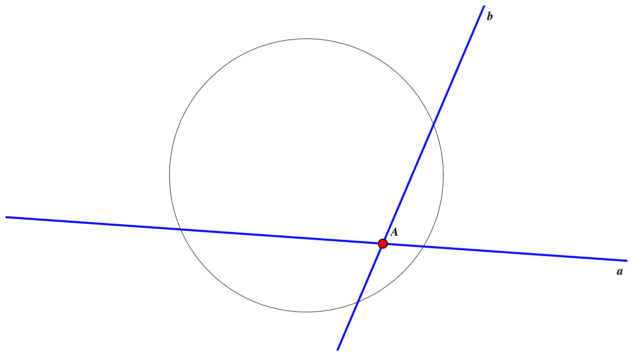
De consistentie van de nieuwe meetkunde (het feit dat de nieuwe meetkunde vrij is van contradicties) werd bewezen met behulp van een model, door de Italiaanse meetkundige Eugenio Beltrami (1835–1900). Beltrami gaf een *interpretatie* van niet-euclidische meetkunde als de meetkunde van een bepaald soort oppervlakken binnen de Euclidische ruimte. De paradoxale eigenschappen van de nieuwe meetkunde worden hier 'waar gemaakt' binnen de Euclidische werkelijkheid, dus we moeten wel concluderen dat de nieuwe meetkunde (letterlijk) net zo consistent is als de oude.

Het model van Beltrami werd later nog enigszins vereenvoudigd door Felix Klein (1849–1925). Het Klein-Beltrami model van de hyperbolische meetkunde bestaat uit een open schijf in het Euclidische vlak. Een open schijf is de oppervlakte van een cirkel, zonder de randen erbij.

Nu gaan we in deze nieuwe wereld de begrippen 'punt', 'incidentie' (dat wil zeggen 'liggen op' of 'snijden'), 'lijn', 'hoek', 'parallel' herinterpreteren (dat wil zeggen: een nieuwe betekenis geven), en wel zo dat de eerste vier postulaten nog steeds opgaan voor deze nieuwe interpretatie van de begrippen die erin voorkomen, maar het vijfde postulaat niet.

Voor de duidelijkheid noemen we een 'lijn' in de nieuwe interpretatie een **lijn**, een 'hoek' in de nieuwe interpretatie een **hoek**, enzovoort.

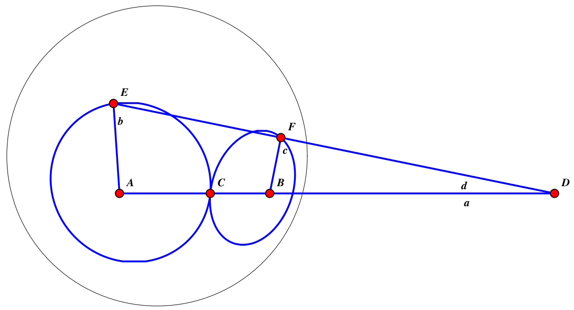
- De **punten** in het Klein-Beltrami model zijn de punten uit het Euclidische vlak die binnen de Klein-Beltrami schijf liggen.



Figuur 3.9: 'Loodrecht staan op' in het Klein-Beltrami model.

- De **lijnen** in het Klein-Beltrami model zijn de open koorden van de Klein-Beltrami schijf, dat wil zeggen de koorden van de cirkelschijf (rechte lijnstukken die twee punten op de cirkel met elkaar verbinden), maar zonder de eindpunten op de cirkel erbij.
- Een **punt** ligt op een **lijn** wanneer het punt op de open koorde ligt.
- Twee **lijnen snijden** elkaar wanneer de twee open koorden een punt gemeenschappelijk hebben.
- Twee **lijnen** a en b staan **loodrecht** op elkaar als één van de volgende twee gevallen zich voordoet (zie Figuur 3.9 en webpagina `LoodrechtKB.html`):
  1. Wanneer minstens één van a en b een middellijn van de schijf is (dat wil zeggen: een lijn door het middelpunt van de schijf), dan staan de **lijnen loodrecht** op elkaar als ze loodrecht op elkaar staan in de gewone Euclidische zin.
  2. Als geen van beide een middellijn is van de schijf dan staat a **loodrecht** op b als de Euclidische lijn die a doortrekt door de *pool* van b gaat (waarbij de pool van b is gedefinieerd als het snijpunt van de raaklijnen aan de schijf door de 'eindpunten' van b).
- Twee **lijnen** zijn **parallel** aan elkaar als de koorden elkaar niet snijden.

Dit herinterpreteren van de Euclidische begrippen lijkt een beetje een goedkope truc. Het is immers nogal wiedes dat als we afspreken om de woorden *lijn* en *parallel* anders te gaan gebruiken, de dingen die we *nu* "parallelle lijnen" noemen heel andere eigenschappen zullen hebben dan *echte* parallelle lijnen. Met name is duidelijk dat er bij bovenstaande herinterpretatie door een gegeven **punt** meerdere **lijnen parallel** zijn aan een gegeven **lijn**.



Figuur 3.10: De Saccheri vierhoek in het Klein-Beltrami model.

Wie dit een goedkope truc vindt heeft de pointe gemist. De pointe is dat het bestaan van modellen waarin postulaten I tot en met IV waar zijn terwijl V onwaar is laat zien dat er in elk "bewijs" van postulaat V uit de postulaten I–IV een fout moet zitten. Immers, als in zo'n bewijs echt alleen maar gebruik is gemaakt van van postulaten I–IV dan zou de conclusie uit dat bewijs moeten gelden in elke situatie waarin postulaten I tot en met IV opgaan, en in de situatie van het Klein-Beltrami model gaat postulaat V juist *niet* op. Het bestaan van het Klein-Beltrami model laat dus zien dat het *onmogelijk* is postulaat V uit de postulaten I–IV af te leiden.

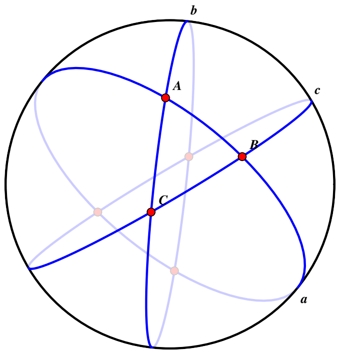
Het construeren van het Klein-Beltrami model bestaat uit het herinterpreteren van een aantal begrippen uit de Euclidische meetkunde, terwijl andere begrippen juist hun oorspronkelijke Euclidische interpretatie houden. **Punten** in het Klein-Beltrami model zijn gewoon punten in het Euclidische vlak waar dat model in ligt. **Lijnen** in het Klein-Beltrami model corresponderen met cirkelkoorden in het Euclidische model. **Snijden van lijnen** in het Klein-Beltrami model correspondeert met snijden van cirkelkoorden in het Euclidische model. Afstand in het Euclidische model correspondeert *niet* met **afstand** in het Klein-Beltrami model. Ook correspondeert de hoek in het Euclidische model niet met de **hoek** in het Klein-Beltrami model. Dit wordt geïllustreerd door de definitie van **loodrecht op elkaar staan** uit het Klein-Beltrami model.

Opdracht 3.3 *Als in het Euclidische vlak twee snijdende lijnen l en m gegeven zijn en P is een punt buiten deze lijnen, dan zal elke lijn door P minstens één van de lijnen l en m snijden. Laat met behulp van een tekening zien dat dit in het Klein-Beltrami model* niet *zo is.*

Opdracht 3.4 *Laat in het Klein-Beltrami model zien: gegeven een* **punt** *en een bf lijn is er een* **loodlijn** *door dat* **punt** *op die* **lijn**. *Aanwijzing: je hebt de definitie van 'loodrecht' in het Klein-Beltrami model nodig.*

Het is instructief om te zien hoe de Saccheri vierhoek zich in het Klein-Beltrami model gedraagt. Zie Figuur 3.10 en de interactieve pagina `SaccheriKB.html` op de website bij dit boek.

3.6 Riemann meetkunde



Figuur 3.11: In het Riemann model snijden alle lijnen.

Zowel Saccheri als Bolyai hadden uit de veronderstelling dat er in een punt buiten een lijn *geen* parallel met een gegeven lijn te vinden is (Saccheri's 'hypothese van de stompe hoek') een tegenspraak afgeleid met de overige aannamen van de Euclidische meetkunde. Als we echter de aanname laten vallen dat lijnen oneindig kunnen worden doorgetrokken volgt er geen tegenspraak, en krijgen we een alternatieve vorm van niet-euclidische meetkunde.

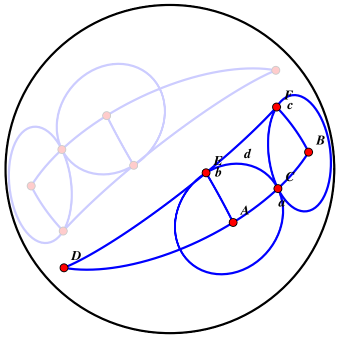
Georg Riemann (1826–1866) zag in dat de 'hypothese van de stompe hoek' geldig wordt zodra we bereid zijn postulaten I, II en V als volgt te herzien:

I' Elk tweetal punten bepaalt minstens één lijn.

II' Een lijn is onbegrensd.

V' Twee lijnen in hetzelfde vlak snijden elkaar altijd.

Hij stelde hiervoor als model een twee-dimensionale wereld voor die bestaat uit het oppervlak van een bol. We definiëren in deze wereld een **rechte lijn** als een grootcirkel van een bol, met de kanttekening dat tegenover elkaar op de bol gelegen punten (polaire punten) worden geïdentificeerd. Een grootcirkel van een bol is een cirkel op het boloppervlak die ontstaat door de bol te snijden met een vlak dat door het middelpunt van de bol gaat. Het is duidelijk dat in zo'n wereld twee **lijnen** elkaar altijd snijden. Immers, twee vlakken door het middelpunt van een bol hebben altijd een lijn l gemeenschappelijk, en de grootcirkels die in die vlakken liggen snijden elkaar in de snijpunten van l met de bol.



Figuur 3.12: De Saccheri vierhoek in het Riemann model.

Door een punt op het boloppervlak buiten een gegeven lijn bestaat dus geen parallel aan die lijn. Zie Figuur 3.11. De figuur maakt duidelijk dat hoe kleiner een driehoek hoe kleiner de afwijking van het Euclidische geval.

Merk op dat een **punt** in de Riemann meetkunde correspondeert met twee tegenover elkaar gelegen punten op de bol. In Figuren 3.11 en 3.12 zie je die tweeling-punten aan de achterkant van de bol als schaduwen.

Opdracht 3.5 *In de Euclidische meetkunde geldt dat twee punten een lijn bepalen: door elk tweetal punten gaat precies één lijn. Dat zou voor Riemann meetkunde ook moeten opgaan. Maar neem de Noord- en de Zuidpool van de Riemann bol: daar gaan oneindig veel verschillende grootcirkels doorheen. Hoe zit dit?*

Opdracht 3.6 *Hoe zou je in de Riemann meetkunde het begrip 'afstand' moeten opvatten?*

Opdracht 3.7 *Wat kun je in de Riemann meetkunde zeggen over de som van de hoeken van een driehoek?*

3.7 Waar deductieve systemen over gaan

Een deductief systeem is een geheel van axioma's en redeneerregels. De postulaten en de redeneerregels van de Euclidische meetkunde kunnen worden opgevat als een deductief systeem. Er zijn twee manieren waarop we tegen de interpretatie en waarheid van deductieve systemen kunnen aankijken: de alledaagse manier en de modeltheoretische manier. We bespreken eerst de alledaagse manier en dan de modeltheoretische manier.

Om de alledaagse manier te introduceren, kijken we eerst naar een bescheiden voorbeeld. Bezie de zin 'Balkenende is minister president van Nederland in 2004'. Laten we die zin *Balkie* noemen. Hoe kijken we nu aan tegen interpretatie en waarheid van Balkie? Simpel: de woorden die in Balkie voorkomen hebben vaste betekenissen. Bijvoorbeeld het woord *Balkenende* slaat op Balkenende. Hierdoor drukt Balkie uit dat Balkenende MP is. Dat is zo, dus Balkie is waar. Nu bekijken we de zin 'de som van de hoeken van een driehoek is 180°'. Laten we die zin *Sommie* noemen. We kunnen nu interpretatie en waarheid van Sommie op dezelfde wijze behandelen als interpretatie en waarheid van Balkie. De woorden in Sommie hebben vaste betekenissen en daardoor gaat Sommie ergens over. Sommie zegt dat voor elke driehoek D geldt dat de som van de hoeken van D gelijk is aan 180°. Daarmee is Sommie een bewering over de werkelijkheid die waar is of onwaar.

Het experiment van de grote wiskundige Karl Friedrich Gauss illustreert deze manier van denken. Gauss (zie bladzijde 101) kwam op het briljante idee om te proberen te toetsen of de werkelijkheid inderdaad Euclidisch is, door metingen te verrichten aan de hoeken van een driehoek die werd gevormd door ver uit elkaar gelegen bergtoppen. De uitkomst van dit meetexperiment was dat de som van de hoeken precies gelijk is aan twee rechte hoeken. Dit kan worden beschouwd als een empirische bevestiging van het feit dat de ons omringende ruimte zich, althans op aardse schaal, Euclidisch gedraagt. Inmiddels weten we (althans, degenen onder ons die natuurkunde hebben gestudeerd) dat de niet-Euclidische aard van de kosmische ruimte pas aan het licht komt als we een schaal van lichtjaren hanteren ...

Opdracht 3.8 *Als je de vraag of de hoeken van een driehoek samen precies gelijk zijn aan* $180°$ *op kosmische schaal gaat toetsen, door de hoeken te meten van een driehoek die gevormd wordt door ons zonnestelsel en twee zeer ver van ons verwijderde sterren, dan doet zich het feit voor dat we altijd rekening moeten houden met een* meetfout. *De grootte van zo'n meetfout laat zich berekenen. Stel dat we weten dat de meetfout hoogstens een boogseconde bedraagt. Een boogseconde is* $1/60$ *van een boogminuut, en een boogminuut is weer* $1/60$ *van een graad. Een fout van een boogseconde op* $180°$ *is dus een fout van* $1/3600$ *graad. Als we nu vinden dat de som van de hoeken van onze kosmische driehoek kleiner is dan* $179°59'59''$ *(*179 *graden,* 59 *boogminuten,* 59 *boogseconden) dan hebben we daarmee empirisch vastgesteld dat de kosmische ruimte hyperbolisch is. Maar stel dat we een som vinden van* $179°59'59\frac{1}{2}''$. *Dan kunnen we* niet *concluderen dat de kosmische ruimte Euclidisch is. Immers, de afwijking van* $180°$ *die we gevonden hebben kan veroorzaakt zijn door de meetfout, maar dat hoeft niet. Het feit dat er altijd een meetfout is lijkt het volgende te betekenen. Een kosmische driehoeksmeting zou tot de conclusie kunnen leiden dat de kosmische ruimte hyperbolisch is, maar zo'n meting kan* nooit *tot de conclusie leiden dat de kosmische ruimte Euclidisch is. Klopt dit? Zo ja, wat is het formele verschil tussen de twee hypothesen 'de kosmische ruimte is Euclidisch' en 'de kosmische ruimte is hyperbolisch'? Geef commentaar.*

De beschreven mannier van kijken naar interpretatie en waarheid van Sommie leidt tot enige twijfels. Willen we deze manier serieus nemen, dan moeten we een *realistische positie* t.o.v. meetkundige objecten innemen. Eénvoudiger gezegd: we moeten er vanuit gaan dat het zin heeft over zaken als driehoeken te praten. Die driehoeken moeten er op één of andere manier zijn. Het is duidelijk dat driehoeken niet precies zulke dingen zijn als Balkenende en bananen. Het zijn —als ze al iets zijn— abstracte aspecten van onze wereld. We zullen hier niet proberen de vraag of er wel of niet driehoeken zijn te beantwoorden. Wel zullen we straks kijken wat er van dit probleem wordt in de modeltheoretische visie.

De modeltheoretische visie werkt zo. We starten met een aantal axioma's. Die axioma's zijn gesteld in woorden. Nu laten we de vaste interpretatie van die woorden los: bijvoorbeeld *lijn* hoeft niet meer per se lijn te betekenen. Stel je nu een of andere keuze van betekenissen van de woorden die in de axioma's voorkomen voor. Als onder die keuze de axioma's waar zijn, dan noemen we die keuze van betekenissen een *model* van de axioma's. Dat klinkt erg abstract, maar het wordt hopelijk duidelijker als we aan het Klein-Beltrami model denken. In dit model wordt het begrip lijn geïnterpreteerd als koorde van een zekere cirkel. Enzovoorts. Je zou kunnen zeggen dat een model zoiets is als een wereld waarin de axioma's waar zijn.

Opdracht 3.9 *Het Klein-Beltrami model wordt gedefiniëerd met behulp van het gewone Euclidische vlak. Maar moeten daar dan niet* punten *gewoon punten zijn en* cirkels *gewoon cirkels?*

Merk op dat in de alledaagse manier van kijken we ons afvragen of de zin over Balkenende overeenstemt met de werkelijkheid. In de modeltheoretische manier van kijken draait de richting zich om: hier vragen we ons af of een model past bij de axioma's.

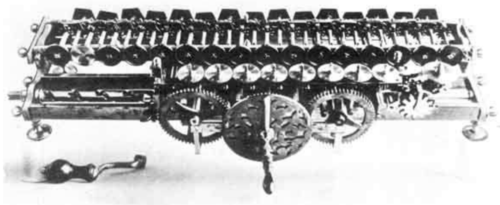
De modeltheoretische manier van kijken heeft groot nut. Het Klein-Beltrami model laat bijvoorbeeld zien dat *als de Euclidische meetkunde een model heeft, dat dan de Hyperbolische Meetkunde ook een model heeft.* Met andere woorden de Hyperbolische Meetkunde is niet minder samenhangend dan de Euclidische Meetkunde. In de modeltheoretische manier van kijken hebben we niet DE MEETKUNDE, maar meetkundes. De vraag wat punten en lijnen nu precies zijn doet er niet meer toe: als de gekozen objecten maar aan de axioma's voldoen.

Lost de modeltheoretische visie nu de kwellende filosofische problemen over het bestaan van mathematische objecten op? Wij denken van niet, en wel om twee redenen. Ten eerste moeten in de modeltheoretische visie aannemen dat er voldoende modellen zijn. Hoe weten we dat? Ten tweede willen we nog steeds over toepassing van de wiskunde kunnen spreken: de vraag naar de waarheid van een meetkundige theorie wordt nu de vraag of bepaalde aspecten van de werkelijkheid een model vormen van de theorie —of wellicht *bij benadering* een model zijn van de theorie. Maar wat betekent het voor de werkelijkheid om een model te zijn van een theorie? Hebben we dan geen ruimtelijke ietsen nodig die de rol van *punt* kunnen spelen?

Concluderend kunnen we zeggen dat wiskundig gezien de modeltheoretische visie de juiste, want vruchtbare, manier van kijken is. Dat betekent echter niet dat modeltheorie ons ook van het filosofische probleem *wat wiskundige objecten zijn* afhelpt.

3.8 Gödel over de grenzen van de axiomatische methode

In 1663 had de filosoof en wiskundige Gottfried Wilhelm Leibniz (1646–1716) aan de Royal Society in Londen een rekenmachine gedemonstreerd die kon vermenigvuldigen.



Leibniz leefde in een tijd waarin geloofd werd dat het hele universum één grote machine was, en hij geloofde zelf heilig in het potentieel van machines. Hij stelde zich ten doel om een universele taal te ontwikkelen voor het formuleren van wetenschappelijke problemen. Vervolgens wilde hij een machine ontwerpen en bouwen die overweg kon met de beweringen uit die universele taal. De bedoeling was dat de machine het al of niet juist zijn van die beweringen zou kunnen bepalen met behulp van logische calculatie. Leibniz droom werd versterkt door de ontdekking van formele systemen die op overtuigende manier de rekenkunde en de meetkunde formaliseerden.

Ach het was een mooie droom ... In 1930/31 liet Kurt Gödel zien dat de droom van Leibniz nooit zou kunnen worden verwezenlijkt. Hij toonde aan dat het redeneersysteem dat achter het gewone basisschool rekenen zit onvolledig is: het is in principe onmogelijk om alle ware beweringen over de natuurlijke getallen te bewijzen. Hier is een iets preciezere formulering. Zij gegeven een redeneersysteem S dat op z'n minst de bescheiden principes voor het gewone basisschool rekenen bevat en dat niet leidt tot tegenspraken.

De axioma's van Peano voor het rekenen met en redeneren over natuurlijke getallen vormen zo'n redeneersysteem. We gebruiken 0 en 1 voor de getallen nul en een, $+$ voor optellen, en $\times$ voor vermenigvuldigen. Voor elk getal n noemen we $n+1$ de *opvolger* van n. De axioma's luiden als volgt:

1. Geen enkel getal heeft 0 als opvolger.
2. Als n ongelijk is aan m, dan is de opvolger van n ongelijk aan de opvolger van m.
3. Voor elk getal n geldt dat $n + 0 = n$.
4. Voor elk tweetal getallen n en m geldt dat $n + (m + 1) = (n + m) + 1$.
5. Voor elk getal n geldt dat $n \times 0 = n$.
6. Voor elk tweetal getallen n en m geldt dat $n \times (m + 1) = n \times m + n$.
7. Voor elke bewering $P(n)$ over n is de volgende bewering een axioma:
   als $P(0)$ geldt en er geldt bovendien voor een willekeurige n dat $P(n + 1)$ volgt uit $P(n)$, dan geldt $P(n)$ voor elk getal n.

Axioma's drie en vier leggen de spelregels voor het optellen vast, en vijf en zes die voor het vermenigvuldigen. Zeven levert een axioma voor elke keuze van $P(n)$. Zeven verwoordt het principe van volledige inductie. Merk op dat machtsverheffen kan worden gedefinieerd in termen van vermenigvuldigen, dus de bewering uit opdracht 2.1 (om maar een voorbeeld te noemen) kan in het redeneersysteem van Peano worden bewezen.

In het redeneersysteem S van Peano kunnen we concreet een ware zin G over getallen aanwijzen die niet door het systeem S bewezen wordt. We kunnen helaas niet onder het probleem uitkomen door die ware zin G aan het gegeven systeem S toe te voegen. Als het resulterende systeem $T = S + G$ nog steeds vrij is van tegenspraak, dan is er een *nieuwe* ware zin H over getallen aan te wijzen die niet volgt uit het verrijkte systeem T. Enzovoorts ...

De conclusie uit Gödel's stelling is dat het weliswaar mogelijk is voor elk welomschreven domein van wiskundig redeneren een formeel systeem te specificeren waarin we het redeneren binnen dat domein getrouw kunnen representeren, maar dat er niet één theorie kan zijn die voor eens en voor altijd werkt voor alle domeinen. In slogan: de wiskundige werkelijkheid is oneindig rijk!

Hoofdstuk 4

Redeneren over Oneindigheid

4.1 Actueel versus potentieel oneindig

Aristoteles maakte in zijn beschouwingen over oneindigheid onderscheid tussen het 'potentieel oneindige' en het 'actueel oneindige'. Met het potentieel oneindige krijg je te maken als je gaat tellen en merkt dat je je tel-proces nooit tot een einde kunt brengen, bij voorbeeld bij het tellen van het aantal punten op een lijnstuk. Met het actueel oneindige krijg je te maken wanneer je een oneindige totaliteit in zijn geheel overziet. Maar kan dat ooit, zo vroeg Aristoteles zich af? Thomas van Aquino, de grote middeleeuwse volgeling van Aristoteles, opperde het volgende bezwaar tegen de notie van een actuele oneindigheid:

> Het bestaan van een actueel oneindige veelheid is onmogelijk. Immers, elke verzameling zaken die men beschouwt moet een specifieke verzameling zijn. En verzamelingen dingen worden gespecificeerd door het aantal dingen dat erin zit. Geen getal is oneindig, want getallen ontstaan door het aftellen van een aantal eenheden. Dus kan geen verzameling dingen inherent of toevalligerwijs onbegrensd zijn.

Als je dit niet helemaal snapt komt dat niet omdat je niet genoeg gevoel voor filosofische diepgang hebt. Wie dit niet snapt kan zichzelf feliciteren, want wat Thomas hier zegt klopt niet. Maar de opvatting dat niets in dit ondermaanse oneindig kan zijn was onder filosofen lange tijd gemeengoed. Het was in de Zestiende Eeuw zelfs uitermate gevaarlijk om iets anders te beweren. Giordano Bruno beweerde dat het universum oneindig is, en Bruno werd om die opvatting (plus nog een aantal andere redelijke en minder redelijke denkbeelden) in 1600 in het openbaar verbrand.

Voor grote wetenschappelijke geesten was oneindigheid lange tijd een harde noot om te kraken. Galileo, ook iemand die het op een gegeven ogenblik met de kerkelijke Inquisitie aan de stok kreeg, beweerde dat redeneren over oneindigheid in termen van groter en kleiner onmogelijk is:

> [...] het totaal van alle (natuurlijke) getallen is oneindig, en het totaal van alle kwadraten is oneindig; en het aantal kwadraten is niet minder dan dat van het

> totaal van alle getallen, en dat laatste aantal is ook niet groter dan het eerste; een en ander laat zien dat de attributen 'gelijk', 'groter' en 'kleiner' niet van toepassing zijn op het oneindige, maar alleen op eindige hoeveelheden.

De filosoof Immanuel Kant (1724–1804) meende (in *Kritik der reinen Vernunft*) dat het actueel oneindige niet kan bestaan omdat het niet kan worden waargenomen:

> [...] om de wereld, die alle ruimte vult, op te kunnen vatten als een een geheel, zou de opeenvolgende synthese van de delen van een oneindige wereld dienen te worden beschouwd als voltooid; dat wil zeggen, met het opsommen van alle coexisterende dingen zou een oneindige hoeveelheid tijd gemoeid moeten zijn.

Wat Kant in feite zegt is dit. Aan het tellen van de elementen van een oneindige verzameling komt nooit een eind. Dus kunnen we zo'n verzameling nooit als een geheel overzien. De werkelijkheid bestaat uit datgene wat we kunnen overzien, en oneindige verzamelingen komen daar dus niet in voor.

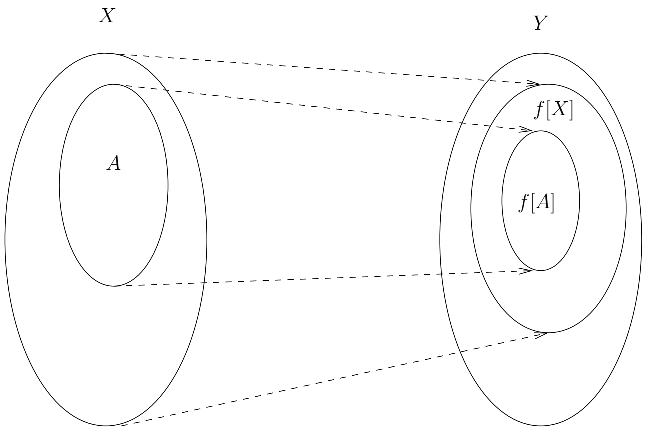
4.2 Afbeeldingen en één-op-één correspondenties

Om uit de impasse te geraken hebben we nieuwe uitleg van het begrip 'even groot' nodig, een uitleg die ook toepasbaar is op oneindig grote verzamelingen.

Laten we even stilstaan bij de fundamentele vraag 'Wat is tellen?' Om in te zien dat het voor tellen van verzamelingen dingen niet absoluut noodzakelijk is om de getallen $1, 2, 3, \ldots$ te gebruiken kijken we naar de manier waarop in oude tijden de herders hun schapen telden. Hoe wist zo'n herder zeker dat 's avonds alle schapen terug waren in de kooi? Die herder had een stapel stenen, en bij ieder schaap dat de kooi binnenging gooide hij een steen van de stapel in een bak. Als bij het laatste schaap dat de kooi binnenging de stapel leeg was wist hij: alle schapen zijn nu binnen, en dan kon hij gerust zijn ogen dicht doen (zoals bekend is schapen tellen de manier bij uitstek om de slaap te vatten). Maar als er een steen over was doolde er nog een schaap door de donkere nacht, en dan moest onze herder er weer op uit. Wat de herder bij het schapen tellen doet is een één-op-één correspondentie aanbrengen tussen de stenen en de schapen. De herder vergewist zich ervan dat schapen en stenen zo aan elkaar kunnen worden gerelateerd dat er bij elk schaap precies één steen hoort. *Welke* steen er aan een bepaald schaap wordt gekoppeld doet er daarbij niet toe. Het bestaan van een één-op-één correspondentie tussen de verzameling schapen en de verzameling stenen betekent: er zijn evenveel schapen als stenen.

Centraal in deze uitleg van 'evenveel' of 'even groot' staat het begrip 'één-op-één correspondentie'. In deze paragraaf leggen we precies vast wat we met een één-op-één correspondentie bedoelen.

Een *afbeelding* of *functie* geeft een recept om elementen van een bepaalde verzameling te associëren met elementen van een (mogelijk andere) verzameling. Een voorbeeld van een functie die reële getallen associeert met andere reële getallen is *kwadrateren* (met zichzelf vermenigvuldigen). Het recept is $x \mapsto x^2$. We kunnen zo'n functie een naam geven, bij voorbeeld f. Dat f een functie is van reële getallen naar reële getallen drukken we uit met $f : \mathbb{R} \to \mathbb{R}$.



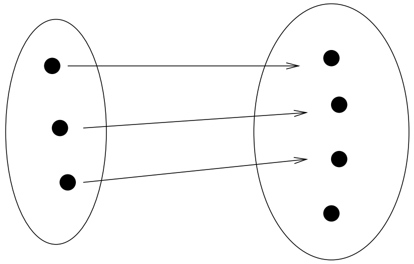
Figuur 4.1: Functie $f : X \to Y$ met beeld $f[X]$ en beeld $f[A]$ van een deelverzameling A van X.

Als f een functie is van X naar Y, en A is een deelverzameling van X, dan kunnen we het beeld van A onder f bekijken. Het beeld van A onder f, notatie $f[A]$, is de verzameling van alle $f(a)$ met $a \in A$. Formeel:

$$f[A] = \{f(a) \mid a \in A\}.$$

De accolades { en } geven aan dat we een verzameling definiëren. Achter | staat de voorwaarde waaraan de elementen uit de verzameling voldoen.

Een functie $f : X \to Y$ heet *injectief* of *één-één* wanneer verschillende elementen van X op verschillende elementen van Y worden afgebeeld.

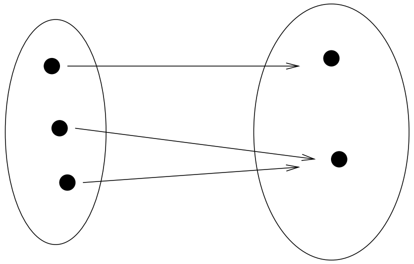


Een injectieve functie wordt een *injectie* genoemd. Om te laten zien dat $f : X \to Y$ injectief is

moet je dus aantonen:

> Als $a \in X$ en $b \in X$, en a en b zijn verschillend, dan zijn ook $f(a)$ en $f(b)$ verschillend.

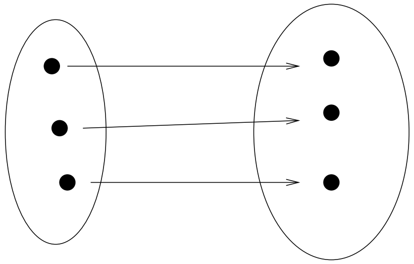
Een functie $f : X \to Y$ heet *surjectief* of *op* wanneer elk element van Y als f-beeld van een of andere $x \in X$ optreedt.



Zo'n functie wordt een *surjectie* genoemd. Om te laten zien dat $f : X \to Y$ surjectief is moet je dus aantonen:

> Als $b \in Y$ dan is er een $a \in X$ met $f(a) = b$.

Een functie $f : X \to Y$ heet *bijectief* (spreek uit: bi-jectief) of een *één-op-één correspondentie* als de functie zowel injectief als surjectief is. De functie $x \mapsto x + 1$ (de opvolgerfunctie) van $\mathbb{N}$ naar $\mathbb{N} - \{0\}$ (van de natuurlijke getallen naar de positieve natuurlijke getallen) is een voorbeeld van een bijectie.



Als $f : X \to Y$ bijectief is is er voor elke $y \in Y$ precies één $x \in X$ met $f(x) = y$. Dat origineel geven we aan met $f^{-1}(y)$.

Opdracht 4.1 *Is de functie 'kwadrateren' op de reële getallen een injectie? Een surjectie? Een bijectie?*

Opdracht 4.2 *Is de functie 'vermenigvuldigen met 2' op de natuurlijke getallen een injectie? Een surjectie? Een bijectie?*

Opdracht 4.3 *Is de functie 'vermenigvuldigen met 2' op de reële getallen een injectie? Een surjectie? Een bijectie?*

4.3 Cantor over oneindigheid

De wiskundige Georg Cantor (1845-1915) nam krachtig stelling tegen de ideeën over oneindigheid van Aristoteles, Thomas van Aquino en Immanuel Kant, door het onderscheid tussen actueel en potentieel oneindig te verwerpen:

> [...] in feite heeft het potentieel oneindige slechts een afgeleid bestaan, in zoverre als een potentieel oneindig begrip altijd terugverwijst naar een logisch daaraan voorafgaand begrip van actuele oneindigheid waar het op berust.

Het aantal elementen dat een verzameling bevat noemen we de *kardinaliteit* van die verzameling. Als een verzameling eindig is is de kardinaliteit van die verzameling een natuurlijk getal. Zo is bij voorbeeld de kardinaliteit van de lege verzameling gelijk aan 0, de kardinaliteit van de verzameling manen van onze planeet is gelijk aan 1, en de kardinaliteit van de verzameling manen van de planeet Jupiter is gelijk aan 4 (tenminste als we 'maan' opvatten als een satelliet van minstens dezelfde orde van grootte als onze eigen maan, anders zijn het er veel meer). Hoe het staat met de kardinaliteit van oneindige verzamelingen was lange tijd (tot ver in de Negentiende Eeuw) een raadsel. Pas rond 1875 liet Georg Cantor zien hoe dit raadsel kan worden opgelost.

Actueel oneindige verzamelingen zijn er volgens Cantor te kust en te keur. Neem het voorbeeld van het vergelijken van de verzameling van natuurlijke getallen met die van de kwadraten van natuurlijke getallen waar Galileo mee worstelde. Volgens Cantor toont het voorbeeld alleen aan dat onze manier van bepalen van de grootte van eindige verzamelingen niet helemaal voldoet voor het bepalen van de grootte van oneindige verzamelingen. Bij tellen van eindige verzamelingen is het telproces op een gegeven moment afgelopen. Wat we daarbij in feite doen is een één-op-één afbeelding maken tussen een verzameling en een beginstuk van de natuurlijke getallen. Zo tellen we de vingers van een hand: duim is een, wijsvinger is twee, middenvinger is drie, ringvinger is vier, en pink is vijf. Dit geeft in feite een één-op-één correspondentie van de vingers en de verzameling $\{1, 2, 3, 4, 5\}$. Die verzamelingen zijn dus even groot.

Met oneindige verzamelingen kan dat even goed. Neem de verzameling van de natuurlijke getallen $\{0, 1, 2, 3, 4, 5, 6, \ldots\}$. Neem aan de andere kant de verzameling van alle kwadraten van natuurlijke getallen $\{0, 1, 4, 9, 16, 25, 36, \ldots\}$. Tussen die verzamelingen bestaat een één-op-één correspondentie, namelijk:

$$\begin{array}{ccc} 0 & \longleftrightarrow & 0 \\ 1 & \longleftrightarrow & 1 \\ 2 & \longleftrightarrow & 4 \\ 3 & \longleftrightarrow & 9 \\ 4 & \longleftrightarrow & 16 \\ 5 & \longleftrightarrow & 25 \\ & \vdots & \end{array}$$

Die verzamelingen zijn dus even groot. Kennelijk kan het bij oneindige verzamelingen voorkomen dat zo'n verzameling even groot is als een van zijn echte deelverzamelingen. Maar dat betekent dat een oude filosofische waarheid, 'het geheel is groter dan het deel,' kennelijk *niet* opgaat voor oneindige verzamelingen. Kwestie van wennen.

4.4 Eindig en aftelbaar oneindig

Met behulp van het begrip *bijectie* is het ook mogelijk een precieze definitie te geven van het begrip *eindige verzameling*. Een verzameling A is eindig wanneer er een natuurlijk getal n is zo dat er een bijectie is tussen A en $\{m \in \mathbb{N} \mid m < n\}$. Met andere woorden: een verzameling is eindig wanneer er een één-op-één correspondentie te vinden is tussen die verzameling en de verzameling $\{0, 1, \ldots, n-1\}$, voor zekere $n \in \mathbb{N}$. De één-op-één correspondentie 'telt' de elementen van de verzameling. Let op: we laten het tellen beginnen by 0. Uit onze definitie van 'eindig' volgt dat $\emptyset$ een eindige verzameling is.

Een verzameling die niet eindig is noemen we *oneindig*. Een oneindige verzameling is dus een verzameling die niet in één-op-één correspondentie gebracht kan worden met een beginstuk van $\mathbb{N}$. Hoe weten we nu dat $\mathbb{N}$ oneindig is? Strikt genomen zou je daarvoor moeten bewijzen dat $\mathbb{N}$ *niet* in één-op-één correspondentie gebracht kan worden met een beginstuk van $\mathbb{N}$. Dit kan door met volledige inductie naar n te bewijzen dat voor elke $n \in \mathbb{N}$ geldt dat er geen bijectie bestaat tussen $\mathbb{N}$ en $\{0, \ldots, n-1\}$, maar zo'n bewijs is alleen voor scherpslijpers.

Twee verzamelingen zijn *even groot* als er een bijectie bestaat tussen die verzamelingen. We gebruiken $A \sim B$ om aan te geven dat er een bijectie bestaat tussen A en B. Verzameling A is *minstens even groot* als B als er een injectie bestaat van B naar A. We gebruiken $B \preceq A$ om aan te geven dat er een injectie bestaat van B naar A.

Een verzameling die even groot is als $\mathbb{N}$ noemen we *aftelbaar oneindig*. Als we toestaan dat een aftelproces eeuwig doorgaat dan kunnen aftelbaar oneindige verzamelingen inderdaad worden afgeteld: het aftelproces is nooit klaar, maar er geldt wel dat elk element $a \in A$ na eindig veel stappen aan de beurt komt bij het aftellen.

De gehele getallen zijn $\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots$. We duiden de verzameling van alle gehele getallen aan met $\mathbb{Z}$. De verzameling $\mathbb{Z}$ is aftelbaar oneindig, want hier is een aftelling van die verzameling:

$$\begin{array}{ccc}
0 & \longrightarrow & 0 \\
1 & \longrightarrow & 1 \\
2 & \longrightarrow & -1 \\
3 & \longrightarrow & 2 \\
4 & \longrightarrow & -2 \\
 & \vdots &
\end{array}$$

Opdracht 4.4 *Laat zien dat het aantal velden van een oneindig schaakbord aftelbaar is.*

Is de verzameling van alle positieve breuken aftelbaar? Op het eerste gezicht lijkt het misschien van niet, want tussen elk tweetal breuken liggen oneindig veel breuken. Cantor liet echter zien dat het wel zo is, met behulp van de volgende elegante opsommingsprocedure:

$$\begin{array}{cccccccccccccc}
0 & \rightarrow & 1/1 & \rightarrow & 1/2 & & 1/3 & & 1/4 & & 1/5 & & 1/6 & \cdots \\
 & & & \swarrow & & \swarrow & & \swarrow & & \swarrow & & \swarrow & & \\
 & & 2/1 & & 2/2 & & 2/3 & & 2/4 & & 2/5 & & 2/6 & \cdots \\
 & & & \swarrow & & \swarrow & & \swarrow & & \swarrow & & & & \\
 & & 3/1 & & 3/2 & & 3/3 & & 3/4 & & 3/5 & & 3/6 & \cdots \\
 & & & \swarrow & & \swarrow & & \swarrow & & & & & & \\
 & & 4/1 & & 4/2 & & 4/3 & & 4/4 & & 4/5 & & 4/6 & \cdots \\
 & & & \swarrow & & \swarrow & & & & & & & & \\
 & & 5/1 & & 5/2 & & 5/3 & & 5/4 & & 5/5 & & 5/6 & \cdots \\
 & & & \swarrow & & & & & & & & & & \\
 & & 6/1 & & 6/2 & & 6/3 & & 6/4 & & 6/5 & & 6/6 & \cdots \\
 & & \text{etc} & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots &
\end{array}$$

Dit is nog niet precies een bijectie, want sommige breuken komen in meer dan een gedaante voor, bij voorbeeld als $1/1$, $2/2$, $3/3$, enzovoorts. Sla de dubbelgangers gewoon over, en je krijgt een bijectie.

Opdracht 4.5 *Kun je een formule in t en n (t voor teller en n voor noemer) bedenken voor de functie die de paren (t, n) precies in de goede volgorde afloopt, zonder de dubbelgangers over te slaan? Om te zien hoe je dit aan moet pakken bekijken we eerst een speciaal geval, zeg de breuk $4/3$. Om het rangnummer van deze breuk te vinden merk je op dat $4/3$ in de aftelling ligt op de diagonaal die volgt op de driehoek met hoekpunten $1/1$, $1/5$ en $5/1$. Na $5/1$ is $4/3$ de vierde breuk op de volgende diagonaal. De driehoek met hoekpunten $1/1$, $1/5$ en $5/1$ bevat de helft van het aantal breuken in de rechthoek met hoekpunten $1/1$, $1/5$, $6/1$ en $6/5$. De breuk $4/3$ heeft dus rangnummer $\frac{5\times 6}{2} + 4 = 19$. Doe nu zelf het algemene geval.*

Goed, we weten nu dat de verzameling van positieve breuken aftelbaar is. Maar dan is zeker ook de verzameling $\mathbb{Q}$ van *alle* breuken aftelbaar. Immers, als de positieve breuken aftelbaar zijn, dan zeker ook de negatieve breuken. Om alle breuken af te tellen nemen we eerst 0, en vervolgens om en om een positieve en een negatieve breuk, gebruik makend van de aftelling f voor positieve breuken die we al hadden. Dus:

$$\begin{array}{ccc}
0 & \longrightarrow & 0 \\
1 & \longrightarrow & f(1) \\
2 & \longrightarrow & -f(1) \\
3 & \longrightarrow & f(2) \\
4 & \longrightarrow & -f(2) \\
 & \vdots &
\end{array}$$

Op dit punt aangekomen in de uitleg over eindig en oneindig is het gebruikelijk een bezoek te brengen aan het zogenaamde Hilbert Hotel. Het Hilbert Hotel, genoemd naar de Duitse wiskundige David Hilbert, is een hotel met aftelbaar oneindig veel kamers.

Opdracht 4.6 *Op een goede dag is het Hilbert Hotel volledig bezet.*

•	•	•	•	•	•	•	•	•	•	···

Dan arriveert er een late gast. Na enig nadenken slaagt de manager er in om deze nieuwe gast onder te brengen. Hoe?

Opdracht 4.7 *We zijn nog steeds bij het Hilbert Hotel, dat nog steeds volledig bezet is. Er arriveert nu een zogenaamde Hilbert bus: een bus met aftelbaar oneindig veel passagiers. De manager slaagt erin om al deze passagiers onder te brengen. Hoe? (Hint: bedenk dat iedere hotelgast een kamernummer heeft, en iedere Hilbert buspassagier een plaatsnummer in de bus. Hoeveel kamers met een even kamernummer zijn er, en hoeveel met een oneven kamernummer?)*

Opdracht 4.8 *Net op het moment dat de portier de deur van het Hilbert Hotel op het nachtslot wil doen (er liggen aftelbaar oneindig veel gasten te ronken in aftelbaar oneindig veel kamers) arriveren er aftelbaar oneindig veel Hilbert bussen, elk met aftelbaar oneindig veel passagiers.*

•	•	•	•	•	•	•	•	•	•	···
•	•	•	•	•	•	•	•	•	•	···
•	•	•	•	•	•	•	•	•	•	···
•	•	•	•	•	•	•	•	•	•	···
•	•	•	•	•	•	•	•	•	•	···
•	•	•	•	•	•	•	•	•	•	···
•	•	•	•	•	•	•	•	•	•	···

$$\vdots$$

Na enig overleg blijkt dat het Hilbert Hotel groot genoeg is om al deze nieuwe gasten onder te brengen. Hoe?

4.5 Overaftelbaar

Zo langzamerhand zou je kunnen gaan denken dat elke oneindige verzameling aftelbaar is. Cantor heeft echter laten zien dat dat niet zo is. $\wp(\mathbb{N})$ is de verzameling van alle deelverzamelingen van natuurlijke getallen. Elementen van $\wp(\mathbb{N})$ zijn bij voorbeeld $\{1, 2\}$ en $\{1, 2, 3\}$. Ook de verzameling E van even natuurlijke getallen en de verzameling $\mathbb{N}$ zijn elementen van $\wp(\mathbb{N})$.

In het algemeen: als X een verzameling is dan is $\wp(X)$ de verzameling van alle deelverzamelingen van X. Cantor liet zien dat de verzameling $\wp(\mathbb{N})$ *niet* aftelbaar is.

Voor het bewijs van "$\wp(\mathbb{N})$ is *niet* aftelbaar" maken we gebruik van het feit dat elke deelverzameling van $\mathbb{N}$ kan worden gerepresenteerd door zijn zogenaamde *karakteristieke functie*. De karakteristieke functie c_A van een deelverzameling A van $\mathbb{N}$ beeldt een natuurlijk getal n af op 1 als n in A zit, en anders op 0. Bij voorbeeld, c_E, de karakteristieke functie voor de even getallen, beeldt elk even getal op 1 af en elk oneven getal op 0. De verzameling van alle karakteristieke functies op $\mathbb{N}$ duiden we aan met $\{0, 1\}^{\mathbb{N}}$.

Het is duidelijk dat de verzameling van karakteristieke functies op $\mathbb{N}$ minstens even groot is als $\mathbb{N}$ zelf. Voor elk getal n is er immers een functie die dat getal op 1 afbeeldt en alle andere getallen op 0, en al die functies zijn verschillend. Dus: er is een injectie van $\mathbb{N}$ naar $\{0, 1\}^{\mathbb{N}}$.

Stelling 4.1 (Diagonaalstelling) *De verzameling* $\{0, 1\}^{\mathbb{N}}$ *is niet aftelbaar.*

Bewijs. Neem aan dat er een aftelling F is van de verzameling $\{0, 1\}^{\mathbb{N}}$. Dit houdt in dat er een oneindige lijst $f_0, f_1, f_2, f_3, \dots$ bestaat van alle karakteristieke functies in $\{0, 1\}^{\mathbb{N}}$. Het volgende plaatje geeft een beeld van hoe die lijst eruit zou kunnen zien. Het plaatje is slechts een voorbeeld; de feitelijke waarden zouden natuurlijk anders kunnen zijn.

	0	1	2	3	4	5	6	$\cdots$
f_0	1	0	0	0	0	0	0	$\cdots$
f_1	0	1	0	1	0	0	1	$\cdots$
f_2	1	0	0	1	1	0	0	$\cdots$
f_3	0	0	0	0	1	1	0	$\cdots$
f_4	1	0	0	0	0	1	1	$\cdots$
f_5	1	0	0	0	0	1	0	$\cdots$
f_6	1	0	0	0	0	0	1	$\cdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\searrow$

Laten we nu eens kijken naar de oneindige reeks van nullen en enen die te zien is op de *diagonaal* in dit plaatje. We definiëren een nieuwe karakteristieke functie f^* door de diagonaal langs te

lopen en alle nullen in enen te veranderen en andersom. Met andere woorden: als $f_n(n) = 1$ dan wordt $f^*(n) = 0$, en als $f_n(n) = 0$ dan wordt $f^*(n) = 1$. Hiermee ligt f^* volledig vast. Als we het voorbeeld uit het plaatje beschouwen zien we:

$$\begin{array}{ll} f_0(0) = 1 & \text{dus } f^*(0) = 0, \\ f_1(1) = 1 & \text{dus } f^*(1) = 0, \\ f_2(2) = 0 & \text{dus } f^*(2) = 1, \\ f_3(3) = 0 & \text{dus } f^*(3) = 1, \\ f_4(4) = 0 & \text{dus } f^*(4) = 1, \\ f_5(5) = 1 & \text{dus } f^*(5) = 0, \\ \text{enzovoort.} & \end{array}$$

Het is duidelijk dat f^* verschillend is van elke f_i. Immers, de waarden van f^* en f_i verschillen voor argument i. Dit is in tegenspraak met de aanname dat de lijst $f_0, f_1, \dots$ een opsomming is van *alle* elementen van $\{0, 1\}^{\mathbb{N}}$. Hiermee is de veronderstelling waar we mee begonnen, namelijk dat er een aftelling F bestaat van de verzameling $\{0, 1\}^{\mathbb{N}}$, weerlegd. ∎

Het is duidelijk waarom dit argument een diagonaal-argument wordt genoemd. Dezelfde redenering kan worden gebruikt om te laten zien dat de verzameling $\mathbb{R}$ van reëele getallen niet aftelbaar is. Wanneer je weet dat elk reëel getal kan worden geschreven in decimale vorm, met oneindig veel cijfers achter de komma, dan kun je voor jezelf nagaan hoe dit werkt.

Hier is nog een kleine finesse. Voor het argument uit de diagonaalstelling is het nodig om te kunnen aannemen dat de decimale representaties uniek zijn, hetgeen wil zeggen dat verschillende representaties verschillende getallen representeren. Die eis kan worden vervuld door oneindige staarten van negens te verbieden. Zonder dit verbod zouden $0,19999\dots$ en $0,2000\dots$ hetzelfde getal (namelijk $\frac{1}{5}$) representeren.

Opdracht 4.9 *Laat zien dat de verzameling van alle* eindige *deelverzamelingen van* $\mathbb{N}$ *aftelbaar is. (Hint: maak gebruik van het feit dat elke niet-lege eindige deelverzameling van* $\mathbb{N}$ *een grootste getal bevat.)*

Opdracht 4.10 *Beschouw de volgende tabel:*

0	*0*	*codeert*	$\emptyset$
1	*1*	*codeert*	$\{0\}$
2	*10*	*codeert*	$\{1\}$
3	*11*	*codeert*	$\{1, 0\}$
4	*100*	*codeert*	$\{2\}$
5	*101*	*codeert*	$\{2, 0\}$
6	*110*	*codeert*	$\{2, 1\}$
7	*111*	*codeert*	$\{2, 1, 0\}$
8	*1000*	*codeert*	$\{3\}$
9	$\dots$	$\dots$	$\dots$

Dit geeft de eerste acht items in de zogenaamde Ackermann codering van eindige deelverzamelingen van natuurlijke getallen als natuurlijke getallen. Leg uit hoe dit werkt. Hoe kun je inzien dat elke eindige deelverzameling van natuurlijke getallen een unieke Ackermann code heeft?

Een verzameling die niet eindig is en niet aftelbaar noemen we *overaftelbaar*. In feite is het bewijs van de overaftelbaarheid van $\{0,1\}^{\mathbb{N}}$ een speciaal geval van een veel algemenere stelling die ook door Cantor werd bewezen, met een bewijs naar hetzelfde stramien.

Stelling 4.2 (Algemene Diagonaalstelling) *Voor geen enkele verzameling A is er een bijectie tussen A en $\wp(A)$.*

Bewijs. Als $A = \emptyset$, dan geldt dat $\wp(A) = \{\emptyset\}$, en $\emptyset$ heeft 0 elementen terwijl $\{\emptyset\}$ één element heeft, dus voor dit geval gaat de stelling op.

Neem nu aan dat $A \neq \emptyset$, en veronderstel dat F een bijectie is tussen A en $\wp(A)$. Nu construeren we een deelverzameling B van A die niet in $F[A]$ zit. Dit gebeurt met de algemene versie van de diagonaliserings-procedure. We definiëren B als volgt:

$$B = \{b \in A \mid b \notin F(b)\}.$$

Met andere woorden: we kiezen voor B de verzameling van alle objecten $b \in A$ die niet in het F-beeld van zichzelf zitten.

We zullen nu laten zien dat deze manier van definiëren B verschillend maakt van alle leden van $F[A]$. Immers, laat C een verzameling in $F[A]$ zijn. Dan is er een $a \in A$ met $F(a) = C$. Nu zijn er twee mogelijkheden: (i) $a \in C$ en (ii) $a \notin C$. In geval (i) geldt dat $a \in F(a)$, en dan volgt uit de definitie van B dat a niet in B zit, in geval (ii) geldt volgens diezelfde definitie dat a juist wel in B zit. In beide gevallen is B dus verschillend van C.

Hieruit volgt meteen dat $B \notin F[A]$, dat wil zeggen: B kan niet het F-beeld kan zijn van enig element van A. Dit is in tegenspraak met onze aanname dat F een bijectie is tussen A en $\wp(A)$. Dus is er geen bijectie tussen A en $\wp(A)$. ∎

Uit Stelling 4.2 plus het feit dat $f : A \to \wp(A)$ gegeven door $f(a) = \{a\}$ een injectie is volgt dat voor elke verzameling A geldt dat zijn machtsverzameling $\wp(A)$ groter is dan A. Dit toont het bestaan aan van het *paradijs van Cantor*: een overvloed van verzamelingen met steeds hogere graden van oneindigheid. Bij voorbeeld: de verzameling $\mathbb{N}$ is aftelbaar oneindig. De verzameling $\wp(\mathbb{N})$ is overaftelbaar. De verzameling $\wp(\wp(\mathbb{N}))$ (die bestaat uit families van getallenverzamelingen) is groter dan $\wp(\mathbb{N})$, en zo gaat dat maar door.

4.6 De stelling van Cantor–Schröder–Bernstein

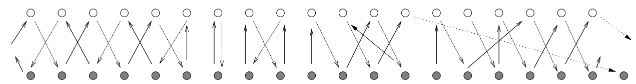
We zullen nu het volgende laten zien: als A minstens even groot is als B en andersom, dan zijn A en B even groot. Dit is geen flauwiteit, want A en B zouden oneindig groot kunnen zijn, een mogelijkheid die we verderop zullen illustreren. Het nu volgende bewijs is van de wiskundigen John Conway en Peter Doyle [2]. We gebruiken $A \preceq B$ voor "er is een injectie van A naar B" en $A \sim B$ voor "er is een bijectie tussen A en B".

Stelling 4.3 (Stelling van Cantor-Schröder-Bernstein) *Als A en B verzamelingen zijn met $A \preceq B$ en $B \preceq A$, dan geldt $A \sim B$.*

Bewijs. Hoewel dit voor het bewijs niet essentieel is nemen we voor het gemak aan dat A en B geen elementen gemeen hebben. We kunnen de verzamelingen immers altijd disjunct maken, bij voorbeeld door A te vervangen door $\{(0,a) \mid a \in A\}$ en B door $\{(1,b) \mid b \in B\}$. Voor wie visueel is ingesteld: we kleuren de elementen uit A wit en die uit B zwart.

We mogen aannemen dat er injecties $f : A \to B$ en $g : B \to A$ zijn. Met behulp van die twee injecties gaan we nu een één-op-één correspondentie tussen A en B construeren.

Daartoe visualiseren we A als een verzameling witte stippen, en B als een verzameling zwarte stippen. De injectie f geven we aan als een verzameling gestippelde pijlen van witte naar zwarte stippen, de injectie g als een verzameling zwarte pijlen van zwarte naar witte stippen.



Laten we de witte stippen even de meisjes noemen, en de zwarte stippen de jongens. Er mogen overaftelbaar veel jongens en meisjes zijn: over de grootte van A en B hebben we niets aangenomen.

Het plaatje geeft dan een huwelijksmarkt te zien, waarbij elke jongen één meisje op het oog heeft, en elk meisje één jongen. Wat we nu moeten laten zien is dat we een massa-huwelijk kunnen sluiten zó dat er geen vrijgezellen of vrijsters overblijven. Elke jongen heeft een meisje op het oog, en elk meisje een jongen, maar het is duidelijk dat de zaak fout gaat als we alle meisjes hun zin geven: er blijven dan vrijgezellen over. Als we alle jongens hun zin geven gaat het trouwens ook fout, want dan blijven er vrijsters over.

Een jongen waar geen meisje verliefd op is noemen we een *sulletje*. Een meisje waar geen jongen verliefd op is is een *tutje*.

Door voorkeurspijlen te volgen krijg je een *pad* door de huwelijksmarkt. Zulke paden zijn er in vier soorten.

1. Paden zonder tutjes of sulletjes die een eindige lus vormen: je begint ergens, bij een jongen of bij een meisje, en na eindig veel stappen van (om en om mannelijke en vrouwelijke) voorkeuren volgen ben je weer bij de oorspronkelijke persoon terug.

$$\begin{array}{ccccccccccc} \circ & \dashrightarrow & \bullet & \to & \circ & \dashrightarrow & \bullet & \to & \circ & \cdots & \bullet \\ \uparrow & & & & & & & & & & \downarrow \\ \bullet & \dashleftarrow & \circ & \leftarrow & \bullet & \dashleftarrow & \circ & \leftarrow & \bullet & \cdots & \circ \end{array}$$

   Een speciaal geval hiervan is natuurlijk $\circ \mathrel{\substack{\dashrightarrow \\ \leftarrow}} \bullet$. Dit komt helaas te weinig voor.

2. Paden zonder tutjes of sulletjes die naar beide zijden oneindig doorlopen. Je komt nooit aan een beginpunt als je achteruit loopt, en nooit aan een eindpunt als je vooruit loopt.

$$\cdots \longrightarrow \circ \dashrightarrow \bullet \longrightarrow \circ \dashrightarrow \bullet \longrightarrow \circ \dashrightarrow \cdots$$

3. Paden die beginnen bij een tutje, en die van daaruit oneindig doorlopen.

$$\circ \dashrightarrow \bullet \longrightarrow \circ \dashrightarrow \bullet \longrightarrow \circ \dashrightarrow \bullet \longrightarrow \circ \dashrightarrow \bullet \longrightarrow \cdots$$

4. Paden die beginnen bij een sulletje, en die van daaruit oneindig doorlopen.

$$\bullet \longrightarrow \circ \dashrightarrow \bullet \longrightarrow \circ \dashrightarrow \bullet \longrightarrow \circ \dashrightarrow \bullet \longrightarrow \circ \dashrightarrow \cdots$$

Meer mogelijkheden zijn er niet. Dat volgt uit het feit dat zowel de voorkeuren van de jongens als die van de meisjes een injectie vormen.

De huwelijksmarkt valt dus in segmenten uiteen, al naar gelang het soort pad dat er doorheen loopt. Maar nu is het gemakkelijk om iedere jongen aan een meisje te koppelen. Bij de eindige segmenten maakt het niet uit wie we hun zin geven: laten we zeggen de meisjes. Bij de oneindige segmenten zonder tutjes of sulletjes maakt het ook niet uit wie we hun zin geven: laten we zeggen de meisjes. Bij de segmenten met een oneindig pad dat begint bij een sulletje moeten we dat sulletje zijn zin geven, anders komt hij nooit aan de vrouw. Maar dan moeten we in dit segment van de huwelijksmarkt *alle* jongens hun zin geven. Bij segmenten met een oneindig pad dat begint bij een tutje moeten we dat tutje haar zin geven, anders vindt ze nooit een vent. Maar dan moeten we in dat segment *alle* meisjes hun zin geven. Dit geeft de gevraagde één-op-één correspondentie. ∎

Dit bewijs beschrijft een procedure om elementen uit A en B één-op-één aan elkaar te koppelen. Die procedure is welomschreven, maar dat betekent niet dat ze altijd met een computer zou kunnen worden uitgevoerd. Stel immers dat we ons bij een gegeven $x \in A$ afvragen aan welke $y \in B$ die x moet worden gekoppeld. Dat hangt ervan af of het pad $g^{-1}(x), f^{-1}(g^{-1}(x)), g^{-1}(f^{-1}(g^{-1}(x))), \ldots$, dat vanaf x terugloopt in eindig veel stappen uitkomt op een element van A of op een element van B. In het eerste geval kunnen we x koppelen aan $f(x)$, in het andere geval moeten we x koppelen aan $g^{-1}(x)$. Maar kijken of een pad eindig of oneindig is geen beslisbare procedure. Als het pad eindig is krijgen we na eindig veel tijd een antwoord. Maar als de vraag na een bepaald eindig tijdsverloop nog niet is beantwoord dan betekent dat nog niet dat het pad oneindig is. Het antwoord "het pad is oneindig" krijgen we *nooit*.

Overigens hebben we in het bewijs geen gebruik gemaakt van het feit dat A en B disjuncte verzamelingen zijn. De relatiemarkt in de *gay scene* verschilt niet wezenlijk van de huwelijksmarkt voor hetero's, dus de stelling gaat ook op als we A en B gelijk nemen, of als we A en B gedeeltelijk laten overlappen.

De stelling van Cantor-Schröder-Bernstein is buitengewoon handig om te laten zien dat er één-op-één correspondenties zijn tussen verzamelingen. Bij voorbeeld: er bestaat een bijectie tussen $[0, 1]$ (alle reële getallen tussen 0 en 1, inclusief de randen), en $[0, 1)$ (alle reële getallen tussen 0 en 1, inclusief de ondergrens 0 maar exclusief de bovengrens 1). Immers, $f : [0, 1] \to [0, 1)$ gegeven door $f(x) = \frac{1}{2}x$ is een injectie, en $g : [0, 1) \to [0, 1]$ gegeven door $g(x) = x$ is ook een injectie. Cantor-Schröder-Bernstein toepassen en klaar.

Laten we voor dit voorbeeld eens in detail nagaan hoe de bijectie h tussen $[0, 1]$ en $[0, 1)$ eruit ziet die we krijgen als we het voorschrift uit het bewijs toepassen.

- Welke punten zitten in een gesloten eindige lus? Alleen het punt 0, want we hebben $0 \xrightarrow{f} 0 \xrightarrow{g} 0$. Dit geeft: $h(0) = 0$.
- Welke punten zitten in een naar beide zijden oneindige rij? Geen.
- Welke punten zitten in een oneindige reeks die met een punt in $[0, 1]$ en een f-stap begint? De punten in het interval $[\frac{1}{2}, 1]$ zijn beginpunt, want een g-voorganger van zo'n punt zit in het interval $[1, 2]$, en dat interval is disjunct van $[0, 1)$. Maar dan zitten ook alle punten in $[\frac{1}{8}, \frac{1}{4}]$ in dezelfde reeks, en alle punten in $[\frac{1}{32}, \frac{1}{16}]$, enzovoorts. De algemene karakterisering is de verzameling punten in een oneindige verzameling intervallen:

  $$X = \bigcup\{[\frac{1}{2 \cdot 4^n}, \frac{1}{4^n}] \mid n \in \mathbb{N}\}.$$

  Hier staat $\bigcup F$ voor de vereniging van een familie F van verzamelingen, dat wil zeggen voor de verzameling van alle elementen die in minstens een verzameling in de familie F zitten.

  Dit geeft: $h(x) = \frac{1}{2}x$ voor $x \in X$.
- Welke punten zitten in een oneindige reeks die met een punt in $[0, 1)$ en een g-stap begint? De punten in het interval $(\frac{1}{2}, 1)$ zijn beginpunt, want een f-voorganger van zo'n punt zit in het interval $(1, 2)$, en dat is disjunct van $[0, 1]$. De algemene karakterisering is de verzameling punten in een oneindige verzameling intervallen.

  $$Y = \bigcup\{(\frac{1}{2 \cdot 4^n}, \frac{1}{4^n}) \mid n \in \mathbb{N}\}.$$

  De punten in Y moeten de beelden worden van h onder de inverse van g. De verzameling originelen wordt dus:

  $$Z = \bigcup\{(\frac{1}{4 \cdot 4^n}, \frac{1}{2 \cdot 4^n}) \mid n \in \mathbb{N}\}.$$

  Het h-voorschrift luidt: $h(x) = 2x$ voor $x \in Z$.

Dit voorschrift voor h is correct, want de verzamelingen $\{0\}$, X, en Z zijn onderling disjunct, en er geldt:

$$[0, 1] = \{0\} \cup X \cup Z.$$

Je ziet dat het specificeren van een bijectie voor een concreet geval nog wel wat voeten in de aarde kan hebben. Zie de volgende opdracht.

Opdracht 4.11 *De functies $f : [0, 1] \to [0, 1)$ gegeven door $f(x) = \frac{1}{2}x$ en $g : [0, 1) \to [0, 1]$ gegeven door $g(x) = x$ zijn injectief. Geef een expliciete definitie van de corresponderende bijectie $h : [0, 1] \to [0, 1)$, naar de specificatie in het bewijs van de Cantor-Schröder-Bernstein stelling.*

Hoofdstuk 5

Recepten voor Bewijs-constructie

In dit hoofdstuk gaan we het hebben over de structuur van eenvoudige bewijzen. Je zult leren structuur in een bewijs aan te brengen, en de structuur in bewijzen van anderen te zien. Het begrip *bewijs* is het centrale begrip in de methode van de formele wetenschappen. Een bewijs is een *tekst* die een argument geeft dat is bedoeld om jezelf en anderen te overtuigen van de waarheid van een bewering. Sommige bewijzen zijn eenvoudig, maar andere zijn kunststukjes die esthetische en intellectuele bevrediging geven. Ze zijn gewoon mooi.

In het dagelijks leven wordt veel geargumenteerd, maar de uitkomst is zelden zonneklaar. Echtelijke ruzies eindigen bij voorbeeld zelden met een volmondig 'jij hebt gelijk' van een van beide partners. Als het zo gemakkelijk zou zijn om uit te maken wie er gelijk heeft hoef je immers geen ruzie te maken. Bij formele wetenschap ligt het anders. De spelregels zijn daar gelukkig veel duidelijker. Meestal ontstaat er geen dispuut over het al of niet correct zijn van een wiskundig bewijs.

Wanneer je een bewijs gaat opschrijven is het een goed idee om heel precies te noteren (i) welke aannamen mogen worden gebruikt in het bewijs (de *gegevens*), en (ii) wat er dient te worden aangetoond (het *te bewijzen*). Dit geeft het volgende schema:

Gegeven: . . .
Te bewijzen: . . .
Bewijs: . . .

Het belangrijkste structuurprincipe is dat bewijzen deelbewijzen kunnen bevatten. We zullen deelbewijzen aangeven door middel van inspringen. De algemene structuur van een bewijs dat een deelbewijs bevat is als volgt:

> *Gegeven:* $A, B, \ldots$
> *Te bewijzen:* P
> *Bewijs:*
> . . .
>
> > *Stel* $C \ldots$
> > *Te bewijzen:* Q
> > *Bewijs:* . . .
> > . . .
> > Dus Q
>
> . . .
> Dus P

Eeen deelbewijs kan natuurlijk zelf ook weer deelbewijzen bevatten:

> *Gegeven:* A, B
> *Te bewijzen:* P
> *Bewijs:*
> . . .
>
> > *Stel* C
> > *Te bewijzen:* Q
> > *Bewijs:*
> > . . .
> >
> > > *Stel* D
> > > *Te bewijzen:* R
> > > *Bewijs:* . . .
> > > . . .
> > > Dus R
> >
> > . . .
> > Dus Q
>
> . . .
> Dus P

De bedoeling van 'Stel' is om een nieuw gegeven toe te voegen aan de lijst van aannamen die mogen worden gebruikt, maar alleen voor de duur van het deelbewijs dat met 'Stel' begint. Als de huidige lijst van gegevens bestaat uit A, B, C, dan zorgt 'Stel D' er dus voor dat die lijst wordt uitgebreid tot A, B, C, D. Hieraan zie je dat het inspringen van belang is om steeds te kunnen bijhouden in welke 'bewijsdoos' je zit.

Bewijzen construeren is een kunst die je door oefening kunt ontwikkelen, net als bij voorbeeld schaken of salsa dansen. Goed schaken is moeilijk, maar de regels van het schaakspel zijn juist heel gemakkelijk. Mooie bewijzen construeren is moeilijk, maar de regels van bewijsconstructie zijn juist heel gemakkelijk. Twee dingen waar je op kunt letten:

1. Hoe gebruik ik een *gegeven*?

2. Hoe ontleed ik een *te bewijzen*?

De beweringen die de *gegevens* en het *te bewijzen* vormen hebben logische structuur. Daar maken we gebruik van om in elk geval te kunnen bepalen wat we moeten doen.

Om de structuur van bewijzen te verduidelijken onderscheiden we in dit hoofdstuk een zevental *logische vormen*, om daarmee beweringen te kunnen onderverdelen in *logische soorten*. Hier is een overzicht van soorten beweringen, met hun logische vorm:

naam	logische vorm	symbool
implicatie	als P dan Q	$\Rightarrow$
conjunctie	P en Q	$\wedge$
equivalentie	P dan en slechts dan als Q	$\Leftrightarrow$
disjunctie	P of Q	$\vee$
negatie	niet P	$\neg$
universele bewering	elke x heeft eigenschap A	$\forall x$
existentie bewering	er is een x met eigenschap A	$\exists x$

In geval van universele beweringen spreken we ook wel van *universele kwantificatie*, in geval van existentie beweringen van *existentiële kwantificatie*.

Als we nu voor al deze gevallen een gebruiksregel (wat doe je met een *gegeven* van deze vorm?) en een introductieregel (hoe toon je een *te bewijzen* van deze vorm aan?) formuleren zijn we klaar.

5.1 Implicatie

Hier is de gebruiksregel voor implicatie. Deze regel wordt ook wel *Modus Ponens* genoemd. Hij geeft aan hoe je een gegeven van de vorm *als P dan Q* kunt gebruiken.

Gegeven: als P dan Q, P
Dus Q.

Bij voorbeeld: uit 'als m oneven is dan is m^2 dat ook' en 'm is oneven' kun je met Modus Ponens concluderen: 'm^2 is oneven.'

En hier is de introductieregel voor implicatie. Deze regel wordt ook wel de deductie regel of de regel voor hypothetisch redeneren genoemd. De implicatie *als P dan Q* wordt bewezen door een deelbewijs te starten met de extra aanname P. Vervolgens wordt met behulp daarvan Q bewezen. Tenslotte wordt het deelbewijs afgesloten met de constatering dat nu *als P dan Q* is bewezen (buiten het deelbewijs).

Gegeven: ...
Te bewijzen: als P dan Q
Bewijs:

> *Stel* P
> *Te bewijzen:* Q
> *Bewijs:* ...

Dus als P dan Q.

De laatste regel, met *Dus als P dan Q* buiten het deelbewijs, wordt overigens vaak weggelaten. De goede verstaander heeft immers al begrepen dat de bedoeling van het deelbewijs was om de implicatie *als P dan Q* aan te tonen.

Een voorbeeld van deze manier van redeneren is het aantonen van de implicatie 'als m oneven is, dan is m^2 ook oneven'. Dat gaat zo:

Te bewijzen: als m oneven is, dan is m^2 ook oneven
Bewijs:

> *Stel* m oneven, dat wil zeggen $m = 2n + 1$.
> *Te bewijzen:* m^2 oneven.
> *Bewijs:* $m^2 = (2n + 1)^2 = 4n + 4 + 1$,
> en dat is oneven.

Hier is een voorbeeld dat zowel gebruik maakt van hypothetisch rederenen als van Modus Ponens.

Gegeven: als P dan Q, als Q dan R
Te bewijzen: als P dan R
Bewijs:

> *Stel* P
> *Te bewijzen:* R
> *Bewijs:* Uit (als P dan Q) en P, concludeer Q.
> Vervolgens, uit (als Q dan R) en Q, concludeer R.

Dus als P dan R

Onthoud: Als het *te bewijzen* de vorm heeft van een implicatie *als P dan Q* dan moet het bewijs beginnen met een nieuw deelbewijs, onder het hoofdje "Stel dat P." Hier is nog een concreet voorbeeld:

Gegeven: m en n zijn natuurlijke getallen.
Te bewijzen: als (m is even en n is even) dan $m + n$ is even.

> Stel dat m en n allebei even zijn.
> Bij voorbeeld, $m = 2p$, $n = 2q$, $p, q \in \mathbb{N}$.
> Dan geldt $m + n = 2p + 2q = 2(p + q)$
> en dus $m + n$ is even.

5.2 Conjunctie

De gebruiksregels voor conjunctie zijn simpel: uit een conjunctie volgt zowel het eerste als het tweede conjunct.

Gegeven: P en Q
Dus P.

Gegeven: P en Q
Dus Q.

De introductieregels voor conjunctie zijn even simpel: een conjunctie volgt door twee gegevens bij elkaar te nemen.

Gegeven: P, Q
Dus P en Q.

5.3 Equivalentie

Een equivalentie *P dan en slechts dan als Q*, vaak afgekort als *P desda Q*, kan worden gezien als een conjunctie van twee implicaties: *(als P dan Q) en (als Q dan P)*.

De behandeling is dus een combinatie van die van 'als dan' en van 'en'.

Gegeven: . . .
Te bewijzen: P desda Q
Bewijs:

Stel P
Te bewijzen: Q
Bewijs: . . .

Stel Q
Te bewijzen: P
Bewijs: . . .

Dus P desda Q.

Als je moet bewijzen dat een reeks van beweringen equivalent is, bewijs je de implicatie van de eerste naar de tweede, van de tweede naar de derde, . . . , en van de laatste naar de eerste. Hier is een voorbeeld. In het voorbeeld speelt het begrip *kleinste gemene veelvoud* een rol. Het kleinste gemene veelvoud (KGV) van twee natuurlijke getallen a en b is het kleinste getal $c \in \mathbb{N}$ met $ap = c, bq = c$, voor zekere $p, q \in \mathbb{N}$. Het KGV bestaat altijd, want ab is een gemeen (=gemeenschappelijk) veelvoud van a en b.

Gegeven: $a, b \in \mathbb{N}$, $a > 0$, $b > 0$.
Te bewijzen: de volgende beweringen zijn equivalent:
(1) a is een deler van b.
(2) a is gelijk aan de grootste gemene deler (GGD) van a en b.
(3) b is gelijk aan het kleinste gemene veelvoud (KGV) van a en b.
Bewijs:
Van (1) naar (2):
Stel a is een deler van b.
Te bewijzen: $\mathrm{GGD}(a, b) = a$.
Bewijs: Uit veronderstelling: er is een $c \in \mathbb{N}$ met $c = \frac{b}{a}$.
Hieruit volgt dat $ac = b$, d.w.z., a is een gemene deler van a en b.
De GGD van a en b kan niet groter zijn dan a, dus $\mathrm{GGD}(a, b) = a$.

Van (2) naar (3):
Stel $\mathrm{GGD}(a, b) = a$.
Te bewijzen: $\mathrm{KGV}(a, b) = b$.
Bewijs: Uit veronderstelling: er is een $c \in \mathbb{N}$ met $ac = b$.
Dus b is een gemeen veelvoud van a en b.
Een gemeen veelvoud van a en b kan niet kleiner zijn dan b, dus $b = \mathrm{KGV}(a, b)$.

Van (3) naar (1):
Stel $\mathrm{KGV}(a, b) = b$.

Te bewijzen: a is een deler van b.
Bewijs: Uit de definitie van KGV: er is een $c \in \mathbb{N}$ met $ac = \mathrm{KGV}(a, b)$.
Met veronderstelling $\mathrm{KGV}(a, b) = b$: er is een $c \in \mathbb{N}$ met $ac = b$.
Dus a is een deler van b.

Opdracht 5.1 *Bewijs dat de volgende drie beweringen equivalent zijn (A en B zijn verzamelingen; $A \subseteq B$ wil zeggen dat elk element van A ook element van B is, $A \cap B$ is de verzameling van dingen die zowel element van A als van B zijn, $A \cup B$ is de verzameling van dingen die element van A of van B zijn, of element van allebei):*

1. $A \subseteq B$.
2. $A \cap B = A$.
3. $A \cup B = B$.

Opdracht 5.2 *Neem aan dat n een natuurlijk getal is. Laat zien dat de volgende beweringen equivalent zijn.*

1. *n is deelbaar door* 3.
2. *$3n$ is deelbaar door* 9.
3. *$n + 3$ is deelbaar door* 3.

De gebruiksregels voor equivalenties zijn simpel; je mag altijd een bewering vervangen door een equivalente bewering:

Gegeven: P desda Q, P, . . .
Dus Q

Gegeven: P desda Q, Q, . . .
Dus P

5.4 Negatie

Introductieregel. Om iets van de vorm *niet* P te bewijzen probeer je uit de aanname P een tegenspraak af te leiden. Een tegenspraak krijg je als je erin slaagt om zowel Q als *niet* Q af te leiden (voor een of andere bewering Q). Als dat lukt onder de aanname P dan klopt er iets niet, en dan is *niet* P kennelijk het geval. Als we $\perp$ gebruiken voor een tegenspraak kunnen we deze regel als volgt opschrijven:

> *Gegeven:* ...
> *Te bewijzen:* niet P
> *Bewijs:*
>
> > *Stel* P
> > *Te bewijzen:* $\perp$
> > *Bewijs:* ...
>
> Dus niet P.

De bewijzen van Stelling 1.1 en 1.2 hebben deze vorm. Figuur 5.1 geeft stelling 1.1 nogmaals, met het bewijs in doos-formaat. De bewering Q waarvoor we de tegenspraak Q samen met *niet* Q afleiden is hier: '$\frac{m}{n}$ is een breuk in eenvoudigste vorm.'

Wanneer *niet* P in het gegeven voorkomt kun je proberen eerst P af te leiden. Wanneer dat lukt kun je uit de combinatie van *niet* P en P concluderen wat je maar wilt:

> *Gegeven:* P, niet P
> Dus Q.

Immers, de combinatie van gegevens 'P, niet P' is zelf al een tegenspraak. Zoiets kan in geen enkele situatie voorkomen. Q concluderen kan de zaak dus niet erger maken dan zij al is.

5.5 Bewijs door contradictie

In schier hopeloze gevallen is een bewijs door contradictie (of: *bewijs uit het ongerijmde*) soms een laatste redmiddel om een bewering P aan te tonen. Dit gaat als volgt: neem extra gegeven *niet* P aan, en laat zien dat daar een contradictie uit volgt. Dan is P kennelijk waar. Dit is de

> *Gegeven:* $x^2 = 2$
> *Te bewijzen:* er zijn geen $m, n \in \mathbb{N}$ met $x = \frac{m}{n}$.
> *Bewijs:*
>
> > *Stel* er zijn $m, n \in \mathbb{N}$ met $x = \frac{m}{n}$.
> > *Te bewijzen:* $\perp$.
> > *Bewijs:*
> > Neem aan dat $x = \frac{m}{n}$ in eenvoudigste vorm is,
> > d.w.z., er zijn geen $k, p, q \in \mathbb{N}$ met $k \neq 1$, $m = kp$ and $n = kq$.
> > Dan geldt: $x^2 = (m/n)^2 = 2$.
> > Dus: $2 = (m/n)^2 = m^2/n^2$.
> > Door beide zijden met n^2 te vermenigvuldigen vinden we: $2n^2 = m^2$.
> > Dus m^2 is even.
> > Kwadraten van oneven getallen zijn altijd oneven, dus m is even.
> >
> > Dus er is een $p \in \mathbb{N}$ met $m = 2p$.
> > Invullen van $2p$ voor m in $2n^2 = m^2$ geeft $2n^2 = (2p)^2 = 4p^2$.
> > Hieruit blijkt dat $n^2 = 2p^2$, dus n is ook even.
> >
> > Dus m en n zijn allebei even.
> >
> > Tegenspraak met de aanname dat m/n een breuk is in eenvoudigste vorm.
> > Dat wil zeggen: $\perp$.
>
> Dus de wortel uit 2 is geen breuk.

Figuur 5.1: Nogmaals Stelling 1.1.

methode die Saccheri gebruikte in zijn poging om het vijfde postulaat van Euclides te bewijzen. In schema:

> *Gegeven:* ...
> *Te bewijzen:* P
> *Bewijs:*
>
> > *Stel* niet P
> > *Te bewijzen:* $\perp$
> > *Bewijs:* ...
>
> Dus P.

Let op: dit is anders dan het bewijs van een negatie. Bij het bewijzen van een negatie nemen we, om *niet* P te bewijzen, aan dat P, in de hoop een tegenspraak af te leiden. Bij een bewijs uit het ongerijmde nemen we, om P te bewijzen, aan dat *niet* P, in de hoop een tegenspraak af te leiden.

Hier is een (curieus) voorbeeld. We laten zien: er zijn irrationale getallen a en b met de eigenschap dat a^b rationaal is. Stel, voor een contradictie, dat dit *niet* zo is. Dat wil zeggen: stel dat voor elk paar van irrationale getallen a en b geldt dat a^b irrationaal is. Beschouw nu het getal $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$. Uit stelling 1.1 weten we dat $\sqrt{2}$ irrationaal is. Dus, met de aanname: $\sqrt{2}^{\sqrt{2}}$ is irrationaal. Uit het feit dat $\sqrt{2}^{\sqrt{2}}$ en $\sqrt{2}$ beide irrationaal zijn volgt, weer met de aanname: $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$ is irrationaal. Maar dit levert een tegenspraak, want $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$, en dat is een rationaal getal.

Let op: op deze manier hebben we nog niet twee irrationale getallen a en b gevonden zodat a^b rationaal is. We hebben alleen bewezen dat dit soort getallen bestaan. Om twee van zulke getallen daadwerkelijk te vinden is een veel sterker bewijs nodig.

5.6 Disjunctie

Een disjunctie volgt uit elk van de disjuncten. De introductieregels luiden dus als volgt:

> *Gegeven:* P
> Dus P of Q.

> *Gegeven:* Q
> Dus P of Q.

Hoe gebruik je een disjunctie als gegeven? Stel dat P *of* Q gegeven is, en je moet R aantonen. Dan laat je zien R zowel uit aanname P als uit aanname Q kan worden afgeleid. In schema:

> *Gegeven:* P of Q, ...
> *Te bewijzen:* R
> *Bewijs:*
>
> > *Stel* P
> > *Te bewijzen:* R
> > *Bewijs:* ...
>
> > *Stel* Q
> > *Te bewijzen:* R
> > *Bewijs:* ...
>
> Dus R.

Soms kunnen we in een redenering gebruik maken van het feit dat P *of niet* P een logische waarheid is. Als we dus zowel uit P als uit niet P conclusie B kunnen afleiden, dan hebben we daarmee B bewezen. Hier is een voorbeeld:

Voor elke $n \in \mathbb{N}$ geldt dat $n(n+1)$ even is.
Bewijs.
  Stel n is even.
  Dan is een van de factoren van $n(n+1)$ even, dus $n(n+1)$ is even.

  Stel n is oneven. Dan is $n+1$ even.
  Weer geldt: een van de factoren van $n(n+1)$ even, dus $n(n+1)$ is even.

Dit heet een bewijs door *gevalsonderscheiding*. Soms moeten meer dan twee gevallen worden onderscheiden. Zie de nu volgende opdracht.

Opdracht 5.3 *Laat zien dat voor elke $n \in \mathbb{N}$ geldt dat $n(n+1)(n+2)$ een drievoud is.*

Het volgende voorbeeld is een variant op het curieuze voorbeeld dat we in 5.5 hebben gezien. Zij $\mathbb{R}$, de verzameling van reële getallen, het discussiedomein, en laat $P(x)$ de volgende eigenschap zijn:

$$x \notin \mathbb{Q} \text{ en } x^{\sqrt{2}} \in \mathbb{Q}.$$

Hier staat $\mathbb{Q}$ voor de verzameling van alle breuken. Met andere woorden, x heeft eigenschap P dan en slechts dan als x geen breuk is, maar $x^{\sqrt{2}}$ is wel een breuk. We zullen nu laten zien dat of $\sqrt{2}$ of $\sqrt{2}^{\sqrt{2}}$ deze eigenschap P heeft.

Er geldt hoe dan ook: $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ of $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$.

Stel $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$.
Dan weten we, omdat $\sqrt{2} \notin \mathbb{Q}$ (Stelling 1.1), dat $\sqrt{2}$ eigenschap P heeft.

Stel $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$.
Dan weten we, omdat $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$, dat $\sqrt{2}^{\sqrt{2}}$ eigenschap P heeft.

Hieruit volgt: $P(\sqrt{2})$ of $P(\sqrt{2}^{\sqrt{2}})$.

5.7 Universele bewering

Wanneer je een universele bewering "voor alle x: $A(x)$" moet bewijzen moet het bewijs altijd beginnen met: "Stel dat c een willekeurig ding is" of "laat c een willekeurig ding zijn." Vervolgens laat je zien dat c voldoet aan $A(c)$, en klaar. De truc is dat je over c niets aanneemt; met name mag c niet eerder in het bewijs gebruikt zijn. Omdat je geen specifieke informatie over c gebruikt geldt wat je bewijst van *elke* c. Het schema wordt dus:

Gegeven: ...
Te bewijzen: Voor elke x: $A(x)$
Bewijs:

> *Stel* c is een willekeurig ding
> *Te bewijzen:* $A(c)$
> *Bewijs:* ...

Dus voor elke x: $A(x)$.

In het geval dat de universele bewering *beperkt* is tot een of andere verzameling D begin je met "stel dat c een willekeurig ding in D is." Het schema wordt dan:

Gegeven: ...
Te bewijzen: Voor elke $x \in D$: $A(x)$
Bewijs:

> *Stel* c is een willekeurig element van D
> *Te bewijzen:* $A(c)$
> *Bewijs:* ...

Dus voor elke $x \in D$: $A(x)$

Je zou je kunnen afvragen wat er bedoeld is met een "willekeurig ding". Bij voorbeeld: wat is een willekeurig natuurlijk getal? Is het groot? Is het klein? Een priemgetal of juist niet? Die zorgen worden veroorzaakt door de gedachte aan specifieke getallen. In feite is "stel dat c een willekeurig element van D is" hetzelfde als tegen de lezer zeggen: "Ik heb een element van D nodig, en het maakt niet uit welk element dat is. Jij mag kiezen. Want welk element jij ook kiest, ik ben in staat om het gevraagde bewijs te leveren."

Een universele bewering komt vaak voor met een implicatie. In dit geval is het volgende schema handig:

Gegeven: ...
Te bewijzen: Voor elke x: als $A(x)$ dan $B(x)$.
Bewijs:

> *Stel* c is een object waarvoor $A(c)$ geldt
> *Te bewijzen:* $B(c)$
> *Bewijs:* ...

Dus voor elke x: als $A(x)$ dan $B(x)$.

Dat was de introductie van een universele bewering. Hoe staat het met het gebruik van een universeel gegeven? Als voor elke x geldt dat $A(x)$ dan geldt $A(t)$ voor elke t die je zou willen kiezen. Dit geeft:

Gegeven: Voor elke x: $A(x)$.
Dus $A(t)$.

In het geval van beperkte universele bewering:

Gegeven: Voor elke $x \in D$: $A(x)$, $t \in D$. Dus $A(t)$.

5.8 Existentie bewering

Om te laten zien dat er een x is die aan $A(x)$ voldoet is het voldoende om een object t te produceren of aan te dragen, en daarvoor te laten laten zien dat $A(t)$ het geval is. In schema:

Gegeven: $A(t)$ Dus, er is een x met $A(x)$.

Dit drukt uit dat elk voorbeeld dat aan A voldoet gebruikt kan worden om "er is een x met $A(x)$" aan te tonen.

Voor beperkte existentiële kwantificatie hebben we natuurlijk een voorbeeld nodig dat aan de beperking voldoet:

Gegeven: $A(t)$, $t \in D$ Dus, er is een $x \in D$ met $A(x)$.

Existentie bewijzen leveren niet altijd een specifiek voorbeeld object op. Stel dat gegeven is dat $P(a)$ of $P(b)$. Uit $P(a)$ volgt dat er een x is met $P(x)$, en uit $P(b)$ volgt dat er een x is met $P(x)$. Maar dan volgt er is een x met $P(x)$ ook uit $P(a)$ of $P(b)$, met de regel voor het gebruik van een disjunctie. Echter, welke van de twee objecten a of b nu aan P voldoet weten we niet. We kunnen dit nog wat concreter maken. Is er een irrationaal getal α met de eigenschap dat $\alpha^{\sqrt{2}}$ een breuk is? Ja, want we hebben hierboven aangetoond dat ofwel $\sqrt{2}$ ofwel $\sqrt{2}^{\sqrt{2}}$ die eigenschap heeft. Het bewijs vertelt ons dus dat er een α moet zijn met de gevraagde eigenschap, maar het vertelt ons niet welke van de twee kandidaten voldoet.

Wanneer je een gegeven van de vorm " er is een x met $A(x)$" wilt gebruiken om een of andere conclusie B te bewijzen moet je altijd starten met: "Stel dat c een object is dat aan A voldoet." Vervolgens probeer je B aan te tonen op basis van deze aanname. In schema:

Gegeven: Er is een x met $A(x)$, ...
Te bewijzen: B
Bewijs:
    Stel c is een object dat aan A voldoet.
    Te bewijzen: B
    Bewijs: ...
Dus B

5.9 Bewijsregels toepassen

We hebben hierboven onderscheid gemaakt in zeven soorten van beweringen: implicaties, conjuncties, equivalenties, disjuncties, negaties, universele beweringen en existentiële beweringen. Als je de beweringen in symbolen opschrijft zijn de beweringen te herkennen aan het logische hoofdsymbool dat ze bevatten: $\Rightarrow$ (implicatie), $\wedge$ (conjunctie), $\Leftrightarrow$ (equivalentie),$\vee$ (disjunctie), $\neg$ (negatie), $\forall$ (universele kwantificatie) of $\exists$ (existentiële kwantificatie). We hebben nu voor elke soort van bewering gezegd hoe je een bewering van die vorm moet *gebruiken* als het een gegeven is, en hoe je een conclusie van die vorm moet *ontleden* om het bewijsprobleem te vereenvoudigen. Dit geeft twee maal zeven is veertien bewijsregels. Een extra bewijsregel voor bewijs door contradictie brengt het totaal op vijftien.

Dit waren alle bewijsregels. Je kunt je voorstellen dat met behulp van deze regels een "formele taal van het bewijzen" kan worden ontwikkeld die geschikt is voor verwerking per computer. Kandidaatbewijzen kunnen dan helemaal formeel worden opgeschreven. Zo'n geformaliseerd bewijs kan vervolgens met de computer worden gecontroleerd. Dit heet: automatische bewijsverificatie. De Nederlandse wiskundige en informaticus Dick de Bruijn was een van de pioniers. Het door hem en zijn groep ontwikkelde programma *Automath* was de eerste automatische bewijschecker die ooit is geconstrueerd. We komen er in Hoofdstuk 6 op terug.

Hier is nog een eenvoudig bewijs over verzamelingen. Als A en B verzamelingen zijn bedoelen we met $A - B$ de verzameling van alle elementen van A die niet in B zitten. Formeel: $A - B = \{a \in A \mid a \notin B\}$. We noemen dit het *verschil van A en B*).

Gegeven: A, B, C zijn verzamelingen.
Te bewijzen: $A - C \subseteq (A - B) \cup (B - C)$.
Bewijs: Laat x een willekeurig object in $A - C$ zijn.
We moeten laten zien dat $x \in (A - B) \cup (B - C)$.

> Neem aan dat $x \in B$. Uit $x \in A - C$ weten we dat $x \notin C$.
> Dus $x \in B - C$.
> Maar dan ook: $x \in (A - B)$ of $x \in (B - C)$.

Dus $x \in (A - B) \cup (B - C)$.

Neem aan dat $x \notin B$. Uit $x \in A - C$ weten we dat $x \in A$.
Dus $x \in A - B$.
Maar dan ook: $x \in (A - B)$ of $x \in (B - C)$.
Dus $x \in (A - B) \cup (B - C)$.

Hier zijn nog wat aanwijzingen voor het aanpakken van eenvoudige bewijsproblemen:

1. Staar je niet blind op het gegeven: pogingen om het gegeven direct om te zetten in de bewering die bewezen moet worden zijn meestal vruchteloos.
2. Concentreer je op hetgeen bewezen moet worden. Aan de logische vorm van de bewering die bewezen moet worden kun je zien wat de eerste stap van het bewijs moet zijn.
3. Probeer je bewijsprobleem te vereenvoudigen. Dat kan bij voorbeeld als volgt:
   - Als je een implicatie *als P dan Q* moet bewijzen, voeg dan P toe aan wat gegeven is en probeer Q te bewijzen.
   - Als je een universele bewering *voor alle x geldt $A(x)$* moet bewijzen, bewijs dan $A(c)$ voor een willekeurig object c.
4. Pas wanneer je op deze manier het bewijsprobleem zoveel mogelijk hebt vereenvoudigd wordt het tijd om naar de gegevens te gaan kijken om te zien welk gegeven je nodig hebt. Dat kan bij voorbeeld als volgt:
   - Als een van de gegevens van de vorm *P of Q* is, en je moet R bewijzen, voeg dan eerst P aan de gegevens toe en probeer R te bewijzen, en voeg daarna Q aan de gegevens toe en probeer R te bewijzen.
   - Als een van de gegevens van de vorm *er is een x met $A(x)$* is, en je moet P bewijzen, geef het object dat aan A voldoet dan een naam c (dat doe je door $A(c)$ aan de gegevens toe te voegen), en bewijs P.
5. Het bewijzen van negaties is in het algemeen lastig. Vaak is het daarom een goed idee om dit zolang mogelijk uit te stellen. Dat kan bij voorbeeld als volgt.
   - Als het te bewijzen van de vorm *niet (P of Q)* is, vervang dit dan door *(niet P) en (niet Q)*. Dit mag omdat de twee beweringen *logisch equivalent* zijn: ze hebben dezelfde logische betekenis.
   - Als het te bewijzen van de vorm *niet (als P dan Q)* is, vervang dit dan door *P en niet Q*. Dit mag omdat de twee beweringen *logisch equivalent* zijn.
   - Als het te bewijzen van de vorm *niet (voor elke x geldt $A(x)$)* is, vervang dit dan door *er is een x met niet $A(x)$*. Dit mag omdat de twee beweringen *logisch equivalent* zijn.
   - Als het te bewijzen van de vorm *niet (er is een x met $A(x)$)* is, vervang dit dan door *voor elke x geldt niet $A(x)$*. Dit mag omdat de twee beweringen *logisch equivalent* zijn.

6. Probeer als het even kan een bewijs uit het ongerijmde te vermijden. Deze bewijsregel is alleen in zeer uitzonderlijke gevallen nodig. Bewijzen uit het ongerijmde hebben als bezwaar dat je je er gemakkelijk in kunt verstrikken. Zelfs als het je lukt om een bewijs uit het ongerijmde te leveren is het achteraf vaak moeilijk om te *zien* waarom het bewijs correct is.

5.10 Bewijzen, tegenvoorbeelden, open problemen

Als je een interessante wiskundige bewering tegenkomt, dan zijn er drie mogelijkheden:

- Je vermoedt dat die bewering waar is.
- Je vermoedt dat de bewering onwaar is.
- Je hebt geen idee of de bewering waar is of niet.

In het eerste geval kun je gaan proberen je vermoeden *hard te maken* door de bewering te bewijzen. In het tweede geval kun je proberen je vermoeden hard te maken door de bewering te weerleggen. In het derde geval heb je kennelijk te maken met een probleem dat je boven de pet gaat, een probleem waar je zelfs geen vage vermoedens over hebt.

Hier is een eenvoudig voorbeeld. De machtsverzameling van een verzameling A is de verzameling van alle deelverzamelingen van A. Formeel $\wp(A) = \{B \mid B \subseteq A\}$. De doorsnede van twee verzamelingen is de verzameling van alle dingen die in beide verzamelingen zitten. Formeel: $A \cap B = \{x \mid x \in A \text{ en } x \in B\}$. Is het nu zo dat voor elk tweetal verzamelingen A, B geldt dat de machtsverzameling van de doorsnede van A en B gelijk is aan de doorsnede van de machtsverzameling van A en de machtsverzameling van B? Formeel: geldt voor alle A, B dat $\wp(A \cap B) = \wp A \cap \wp B$?

Allereerst: hoe kom je aan een vermoeden over deze kwestie? Gewoon, door simpele gevallen uit te proberen. Neem $A = \{1, 2\}$ en $B = \{2, 3\}$. Dan is $\wp A = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ en $\wp B = \{\emptyset, \{2\}, \{3\}, \{2, 3\}\}$. De doorsnede van deze twee machtsverzamelingen is $\{\emptyset, \{2\}\}$. Dat is gelijk aan de machtsverzameling van $\{2\}$, een dat is weer de doorsnede van A en B. Dat ziet er veelbelovend uit. Eens kijken of we het kunnen bewijzen.

Om te bewijzen dat twee verzamelingen aan elkaar gelijk zijn moeten we twee dingen laten zien: (1) elk element van de eerste verzameling zit in de tweede verzameling, (2) elk element van de tweede verzameling zit in de eerste verzameling. Het bewijs van $\wp(A \cap B) = \wp A \cap \wp B$ ziet er dus zo uit:

Te bewijzen: Voor elk tweetal verzamelingen A, B: $\wp(A \cap B) = \wp A \cap \wp B$.
Bewijs: Laat A, B willekeurige verzamelingen zijn.

We laten eerst zien dat $\wp(A \cap B) \subseteq \wp A \cap \wp B$.
Laat $X \in \wp(A \cap B)$. Dan $X \subseteq A \cap B$.
Dus $X \subseteq A$ en $X \subseteq B$.
Dus $X \in \wp A$ en $X \in \wp B$.

Maar dan ook: $X \in \wp A \cap \wp B$.

Nu laten we zien dat $\wp A \cap \wp B \subseteq \wp(A \cap B)$.
Neem aan dat $X \in \wp A \cap \wp B$.
Dan $X \in \wp A$ en $X \in \wp B$.
Dus $X \subseteq A$ en $X \subseteq B$.
Hieruit volgt dat $X \subseteq A \cap B$.
Maar dat betekent dat $X \in \wp(A \cap B)$.

Opdracht 5.4 *De vereniging van twee verzamelingen A en B is de verzameling van alle dingen die in A of in B zitten (of desnoods in allebei). Formeel: $A \cup B = \{x \mid x \in A \text{ of } x \in B\}$. De vraag is: geldt dat $\wp(A \cup B) = \wp A \cup \wp B$? Geef een bewijs of een tegenvoorbeeld.*

In het algemeen zijn er als je een wiskundige bewering onderzoekt drie mogelijkheden:

- Je slaagt erin de bewering te bewijzen. De bewering is dus een wiskundige stelling.
- Je slaagt erin de bewering te weerleggen door het geven van een *tegenvoorbeeld*. De bewering is daarmee een weerlegd vermoeden.
- Noch het een, noch het ander. Dit kan betekenen dat je een zogenaamd *open probleem* uit de wiskunde bij de kop hebt. Zulke open problemen zijn er te over, Maar het kan natuurlijk ook dat je net niet slim genoeg bent geweest, en dat een andere wiskundige er wel in geslaagd is voor de bewering een bewijs of weerlegging te vinden.

Een voorbeeld van een bewering die met een tegenvoorbeeld kon worden weerlegd was de claim van Pierre de Fermat dat alle natuurlijke getallen van de vorm $2^{2^n} + 1$ priemgetallen zijn. Zie bladzijde 28. En hier zijn een paar voorbeelden van open vragen (vragen waar, op het moment dat dit boek ter perse gaat, geen enkele wiskundige het antwoord op weet) over priemgetallen:

- Een priem-paar is een paar van getallen $(p, p+2)$ met de eigenschap dat zowel p als $p+2$ priemgetallen zijn. Voorbeelden van priem-paren zijn:

  $$(3,5), (5,7), (11,13), (17,19), (29,31), (41,43), (59,61), (71,73), (101,103), (107,109),$$

  $$(137,139), (149,151), (179,181), (191,193), (197,199), (227,229), (239,241), (269,271).$$

  De vraag *Is er een grootste priem-paar?* is een open vraag.

- Een Mersenne priemgetal is een priemgetal van de vorm $2^p - 1$, waarbij p ook een priemgetal is. De vraag *Is er een grootste Mersenne priemgetal?* is een open vraag. Er worden met behulp van computers steeds grotere Mersenne priemgetallen gevonden (google naar GIMPS = "Great Internet Mersenne Prime Search" op het Internet als je aan die zoektocht wilt meedoen), maar een bewijs dat er oneindig veel Mersenne priemgetallen zijn is nooit door iemand geleverd.

- In een brief van Goldbach aan Euler (uit 1747, later dus dan de brief die op bladzijde 28 ter sprake kwam) stond een suggestie die er ruwweg op neerkwam dat elk even natuurlijk getal groter dan twee de som is van twee priemgetallen. Bij voorbeeld: $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 5+5$, $12 = 5+7$, maar ook: $10.000 = 59 + 9941$, $100.000 = 11 + 99989$ $1048576 = 3 + 1048573$. Let wel, het even getal mag op meerdere manieren als som van twee priemen te schrijven zijn. Voor $1048576 = 2^{20}$ zijn er bij voorbeeld heel veel meer mogelijkheden:

  $$(3+1048573), (5+1048571), (17+1048559), (59+1048517), (233+1048343), (359+1048217),$$

  $$(383+1048193), (449+1048127), (563+1048013), (569+1048007), (587+1047989),$$

  enzovoort. Of Euler daarvoor een bewijs wist. Dat wist Euler niet, en tot op de dag van vandaag zijn er geen tegenvoorbeelden gevonden, maar is er ook geen bewijs geleverd.

Wanneer er een open probleem met een lange geschiedenis wordt opgelost, zoals bij voorbeeld gebeurde toen Andrew Wiles de laatste stelling van Fermat bewees (zie blz. 106), dan is dat groot wetenschappelijk nieuws.

Hoofdstuk 6

Bewijzen Vinden en Bewijzen Verifiëren

6.1 Het verschil tussen vinden en verifiëren

Er is een groot verschil tussen de *presentatie* van een bewijs dat je eenmaal hebt en het *vinden* van een bewijs. Vinden van bewijzen heeft te maken met creativiteit en het genereren van inzichten. Stel, je wordt geconfronteerd met een probleem waar je het antwoord niet direct op weet. Wat doe je? Hoe pak je het aan? De kunst van het vinden heet *heuristiek*. "Eureka!", "Ik heb het gevonden!", riep de blote Archimedes toen hij ineens in een flits het principe van de opwaartse druk doorzag, en begreep waarom voorwerpen onder water lichter lijken dan boven water. Zijn methode: rustig in bad gaan zitten en zijn probleem overdenken.

Het onderscheid tussen bewijzen vinden en bewijzen verifiëren was door Aristoteles al heel duidelijk verwoord. Als iemand hem een bewijs zou laten zien, zei hij, dan zou hij zeker in staat zijn om na te gaan of dat bewijs correct was of niet. Dat was immers gewoon een kwestie van nagaan dat de bewering die bewezen werd inderdaad volgde uit de axioma's en primitieve begrippen die in het bewijs werden gebruikt. Maar stel nu dat iemand hem een bewering gaf waar een bewijs van bestond, maar zonder dat bewijs erbij te geven. Dan zou hij niet altijd in staat zijn om zelf het bewijs te leveren. Waar het op neerkomt is dat het nagaan of een bewijs klopt een kwestie is van simpele regels volgen, terwijl het vinden van een bewijs een zaak is waar inspiratie en inventiviteit aan te pas kunnen komen. Het vinden van bewijzen is wezenlijk moeilijker dan het verifiëren van bewijzen.

6.2 Advies van Georg Pólya

De Hongaarse wiskundige Georg Pólya (1887–1985) heeft uitvoerig geschreven over de kunst van het vinden. Uit zijn boek *How to solve it?* ("Hoe los ik het op?" [15]) volgt hier een samenvatting van zijn aanbevelingen:

1. **Het probleem begrijpen** Om meer begrip te krijgen van wat de vraagstelling inhoudt kun je de volgende vragen stellen en de volgende dingen doen:
   - Wat is de onbekende? Wat zijn de gegevens? Wat is de voorwaarde?
   - Is het mogelijk om aan de voorwaarde te voldoen? Is de voorwaarde voldoende om de onbekende te bepalen? Of is het vervuld zijn van de voorwaarde daarvoor niet genoeg? Is de voorwaarde misschien redundant? Of zelfs contradictoir?
   - Maak een tekening. Voer geschikte notatie in.
   - Ontleed de voorwaarde in onderdelen. Kun je ze opschrijven?
2. **Een plan maken** Het gaat er nu om de verbinding tot stand te brengen tussen de gegevens en de onbekende. Het zou kunnen zijn dat je eerst deelproblemen moet aanpakken als de link tussen gegevens en onbekende niet meteen ziet. Uiteindelijk moet je tot een plan komen om de oplossing te vinden. Dit zijn vragen die je jezelf kunt stellen:
   - Heb je het probleem eerder gezien? Of ben je hetzelfde probleem misschien in een iets andere vorm tegengekomen?
   - Ken je een verwant probleem? Ken je een stelling die bruikbaar zou kunnen zijn?
   - Kijk naar de onbekende! En probeer een bekend probleem te vinden met dezelfde onbekende, of met een soortgelijke onbekende.
   - Hier is een probleem dat lijkt op dat van jou, en hier zie je hoe het wordt opgelost. Kun je dat gebruiken? Kun je het resultaat gebruiken? Kun je de methode gebruiken? Moet er misschien een hulpelement worden ingevoerd dat je in staat stelt om het probleem te gebruiken?
   - Hoe zou je het probleem in andere woorden omschrijven? Kun je het nog anders omschrijven? Ga terug naar de definities.
   - Als je er niet in slaagt het probleem dat voor je ligt op te lossen dan kun je proberen eerst een verwant probleem op te lossen. Kun je een verwant probleem bedenken waar je meer vat op hebt? Een algemener probleem? Een analoog probleem? Kun je misschien een deel van het probleem oplossen? Hou vast aan een deel van de voorwaarde, en laat de rest vallen. In hoeverre is de onbekende nu nog bepaald? Hoe kan de onbekende nu variëren? Kun je iets nuttigs afleiden uit de gegevens? Kun je extra gegevens bedenken die nuttig zouden kunnen zijn om de onbekende te bepalen? Kun je de onbekende of de gegevens, of desnoods allebei, op zo'n manier veranderen dat de nieuwe onbekende en de nieuwe gegevens dichter bij elkaar liggen? Heb je alle gegevens gebruikt? Heb je de hele voorwaarde gebruikt? Heb je rekening gehouden met alle essentiële begrippen die in het vraagstuk een rol spelen?
3. **Het plan ten uitvoer brengen** Voer je plan uit. Terwijl je dat doet moet je elke stap controleren. Kun je duidelijk inzien dat de stap correct is? Kun je bewijzen dat de stap correct is?
4. **Terugblik** Onderzoek de verkregen oplossing. Kun je de redenering checken? Kun je de oplossing ook op een andere manier afleiden? Kun je de oplossing (nu achteraf) in één oogopslag zien? Kun je het resultaat of de methode gebruiken voor andere problemen?

Dit zijn de vragen die wiskundigen zichzelf stellen wanneer ze worstelen met een probleem. Imre Lakatos (1922–1974), een Hongaarse wiskundige en filosoof, kwam met de denkbeelden van Pólya in aanraking toen hij *How to solve it?* in het Hongaars vertaalde. Na de Hongaarse opstand van 1956 vluchtte hij naar Cambridge en voltooide daar zijn proefschrift *Proofs and Refutations* (*Bewijzen en Weerleggingen*), waarin hij de gedachte ontwikkelde dat de ontwikkeling van de wiskunde met horten en stoten gaat. Wiskundigen maken voortdurend riskante gissingen die ze dan vervolgens proberen te bewijzen. Soms lukt dat, maar vaak ook niet. Kritiek is in de wiskunde altijd vernietigend: de meest dodelijke manier om een gissing te bekritiseren is door het geven van een tegenvoorbeeld.

6.3 Bewijsverificatie met de computer

Het doel van het *Automath* systeem, waaraan de Nederlandse wiskundige Dick de Bruijn en zijn groep in Eindhoven in 1967 begonnen te werken, was het ontwikkelen van een raamwerk om wiskundige theorieën in uit te drukken. De representatie moest geschikt zijn om de correctheid ervan door een computer te kunnen laten verifiëren. De Bruijn stelde zich op het standpunt dat wat volkomen correct was verwoord correct behoorde te zijn. Een andere norm voor correctheid is er niet, volgens hem.

Automath is gebaseerd op de zogenaamde *getypeerde lambda calculus*. In termen daarvan worden begrippen als “definitie”, “stelling”, “bewijs” en “axioma” gespecificeerd. Een volledig wiskundeboek is gestructureerd als een verzameling van in elkaar geschoven dozen, precies om de manier waarop in Hoofdstuk 5 een bewijs was opgebouwd uit geneste dozen met deelbewijzen. Openen van een doos gebeurt met de introductie van een variabele met een type-declaratie, bij voorbeeld: “Zij x een variabele van type *natuurlijk getal*.” Zulke variabelen kunnen echter ook staan voor wiskundige bewijzen. Volgens De Bruijn maakt het geen verschil of je naar een getal of naar een bewijs verwijst, want het mechanisme dat er achter zit is hetzelfde. Dit heet: “bewijzen gebruiken als objecten” (“proofs as objects”). In een recente terugblik op het Automath project merkt De Bruijn op:

> Het Automath systeem heeft nooit de pretentie gehad om het bedenken van wiskunde te automatiseren, en zelfs niet om de constructie van bewijzen van gegeven stellingen te automatiseren. De Automath correctheids-checker is niets meer of minder dan een uiterst zorgvuldige lezer van goed-gepresenteerd voltooid wiskundig materiaal.

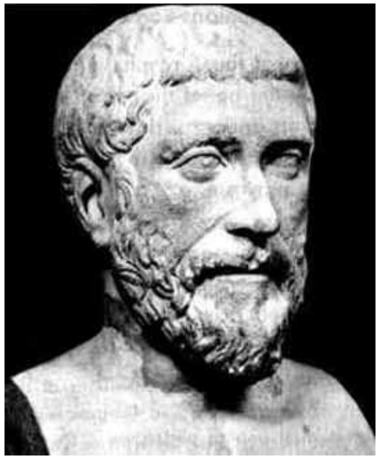
Intussen zijn *proof assistants*, programma’s die bewijzen kunnen verifiëren en die ook (in beperkte mate) kunnen helpen bij het vinden van bewijzen, te kust en te keur op het internet te vinden.

The Coq proof assistant (zie `http://coq.inria.fr`) is zo’n programma. Met behulp van Coq kun je interactief (in interactie met het systeem) bewijzen ontwikkelen.

Biografieën

Bron: *MacTutor History of Mathematics archive*: `http://www-history.mcs.st-andrews.ac.uk/history/`.

Pythagoras van Samos (± 569 vC tot ± 474 vC)



Wat we over Pythagoras weten is uit de tweede hand: er zijn geschriften van hem bewaard gebleven. Pythagoras was wat wij nu een *guru* zouden noemen. Hij had zijn eigen school voor wiskunde, filosofie en spiritualiteit in Croton in Zuid-Italië. De volgelingen die met hem in de *ashram* woonden hadden geen persoonlijke bezittingen, aten strikt vegetarisch, en waren gehouden aan tal van regels. Ze onderschreven overtuigingen zoals de volgende: "Op het diepste niveau is de hele werkelijkheid gebaseerd op wiskunde." "Filosofie wijst de weg naar spirituele verheffing." "Bepaalde symbolen (met name: getallen) hebben een mystieke betekenis."

De school van Pythagoras leek dus in de verste verte niet op een wiskunde faculteit aan een Westerse universiteit. In één opzicht was Pythogoras zijn tijd ver vooruit: lidmaatschap van zijn school stond open voor mannen en vrouwen. De Pythagoreërs leverden belangrijke bijdragen aan de muziektheorie. Ze ontdekten dat trillende snaren met elkaar in harmonie zijn wanneer hun lengten zich tot elkaar verhouden als gehele getallen. De stelling van Pythagoras was al aan de Babyloniërs bekend, maar het is mogelijk dat de Pythagoreërs de eersten waren die er een bewijs voor hadden.

Euclides (± 325 vC tot ± 265 vC)

Euclides van Alexandrië is dan misschien wel niet de grootste wiskundige uit de oudheid, hij is zeker een beroemd wiskundedocent. Hij dankt zijn bekendheid aan *De Elementen*, eeuwenlange *bestseller* als wiskunde-leerboek. Dit boek maakt Euclides tot de belangrijkste wiskundeleraar van alle tijden. Van Euclides' leven is weinig bekend, behalve dan dat hij doceerde in Alexandrië in Egypte.

De *Elementen* is in feite een compilatie van wat er in de Oudheid aan wiskunde bekend was. Originele resultaten van Euclides zitten er waarschijnlijk niet bij, maar de presentatie en organisatie van het materiaal zijn van hem. De *Elementen* begint met definities en de beroemde vijf postulaten. Het vijfde postulaat is (equivalent aan) het zogenaamde parallellenpostulaat: door een punt buiten een lijn kan precies een lijn worden getrokken die parallel is aan die lijn. De beslissing van Euclides om hier een postulaat van te maken leidde tot wat we nu Euclidische meetkunde noemen. Pas in de Negentiende eeuw werd voorgesteld om dit postulaat te laten vallen. Dit leidde tot de studie van niet-Euclidische meetkundes.

Pierre de Fermat (1601–1665)

Fermat was een Franse jurist. Ondanks het feit dat hij de wiskunde slechts als liefhebberij beoefende wordt hij beschouwd als een van de grootste wiskundigen van alle tijden. Het bekendst is hij om zijn werk in de getaltheorie. *Fermat's laatste stelling* is de bewering die Fermat neerkrabbelde in de marge van een boek over rekenkunde van Diophantus: de vergelijking $x^n + y^n = z^n$ heeft geen gehele oplossingen voor $n > 2$. Fermat's opmerking in de marge luidde:

> Ik heb een werkelijk opzienbarend bewijs voor deze stelling ontdekt, maar deze marge is helaas te smal om dat hier te kunnen opschrijven.

Drie eeuwen lang hebben wiskundigen zich suf gepiekerd. Dat nadenken over Fermat's laatste stelling leverde wel allerlei nieuwe interessante wiskunde op, zoals de theorie van commutatieve ringen, maar geen bewijs. Niemand gelooft vandaag de dag dat Fermat echt een bewijs had, al

zullen we dat nooit helemaal zeker weten. Fermat's laatste stelling werd pas in 1994 bewezen door Andrew Wiles.

Leonhard Euler (1707–1783)

Euler was als toegepast wiskundige in dienst van Catharina de Grote. Hij was actief op tal van gebieden: cartografie, organisatie van wetenschappelijke opleidingen, magnetisme, brandweerwagens, machines, scheepsbouw. Al die zaken hadden met wiskunde te maken, en hij werkte aan allerlei onderwerpen tegelijkertijd: getaltheorie (hij bewees Fermat's laatste stelling voor het speciale geval van $n = 3$), infinitesimaalrekening, differentiaalvergelijkingen, calculus, mechanica. Euler werd de grondlegger van de mathematische analyse.

Euler had een zwakke gezondheid, en werd op latere leeftijd geheel blind. Dit belette hem niet om door te gaan met zijn wiskundeonderzoek. Het grootste deel van zijn wetenschappelijke productie kwam tot stand toen hij niet meer kon zien, en zijn werk moest dicteren aan assistenten die hij en passant opleidde tot wiskundigen.

Euler was wat we nu een workaholic noemen. Hij is de meest productieve wiskundige aller tijden. Na zijn dood in 1783 ging de Academie van Sint Petersburg nog zo'n vijftig jaar door met het publiceren van zijn nooit eerder openbaar gemaakte wiskundige manuscripten.

Karl Friedrich Gauss (1777–1855)

Toen Karl Friedrich Gauss op zevenjarige leeftijd naar de lagere school ging werd vrijwel meteen duidelijk dat het onderwijzend personeel te maken kreeg met een ventje met uitzonderlijk talent. De leerlingen moesten rekenen leren, en ze kregen de opdracht om de som van de getallen van 1 tot en met 100 uit te rekenen. De jonge Gauss zag meteen dat die som gelijk was aan 50 paren met elk een som van 101, en hij had onmiddellijk het antwoord: 5050.

Gauss werd een beroemd wiskundige, maar hij hield ervan wiskunde practisch toe te passen, in astronomie, landmeting, en onderzoek naar aardmagnetisme. Later bekwaamde hij zich op het gebied van financiën, en slaagde erin een aardig kapitaal te vergaren door handig investeren in aandelen.

Rond 1800 raakte Gauss geïnteresseerd in de mogelijkheid van niet-Euclidische meetkunde. Hij besprak dit onderwerp uitvoerig met zijn vriend Farkas Bolyai (de vader van János Bolyai), en in correspondentie met collega's. In een boekbespreking uit 1816 overwoog hij de mogelijkheid

van het bewijzen van het parallellenaxioma uit de andere Euclidische axioma's. Die bespreking suggereerde dat hij geloofde in het bestaan van niet-Euclidische meetkunde. Gauss liet aan collega's doorschemeren dat hij vreesde voor zijn reputatie als hij dit in het openbaar zou toegeven.

János Bolyai (1802–1860)

János Bolyai werd geboren in Transylvanië, destijds onderdeel van het Habsburgse keizerrijk, nu in Roemenië. Bolyai leerde wiskunde van zijn vader. Hij werd tevens een bekwaam violist. Na zijn studie ging hij het leger in als genieofficier. Hoewel hij de beste schermer en danser was van het Keizerlijk leger, bleef hij een buitenbeentje: hij rookte of dronk niet.

Tussen 1820 en 1823 werkte hij aan een verhandeling over een volledig systeem van niet-Euclidische meetkunde. Toen hij het wilde publiceren kwam hij erachter dat Gauss hem was voor geweest, maar zijn resultaten nooit openbaar had gemaakt. In 1832 verscheen het werk van Bolyai als appendix bij een verhandeling van zijn vader. In 1848 ontdekte Bolyai dat Lobachevsky in 1829 iets zeer vergelijkbaars had gepubliceerd.

Georg Cantor (1845–1918)

Georg Cantor werd in Sint Petersburg geboren als zoon van een succesvol koopman. Zijn vader wilde aanvankelijk dat hij ingenieur werd, maar stemde toe toen Georg verzocht om over te mogen stappen op wiskunde. Cantor hield zich oorspronkelijk bezig met getaltheorie en analyse. In 1873 liet hij zien dat de rationale getallen aftelbaar zijn, dat wil zeggen dat ze in één-op-één verband kunnen worden gebracht met de natuurlijke getallen. Hij liet ook zien dat de algebraische getallen (getallen die de wortels zijn van polynoomvergelijkingen met gehele coëfficiënten) aftelbaar zijn. Lastiger bleek de vraag of de reële getallen aftelbaar zijn, maar Cantor slaagde erin om te laten zien dat dat niet zo was.

Tussen 1879 en 1884 publiceerde Cantor een reeks van zes artikelen in *Mathematische Annalen* met als doel de grondslag te leggen voor de verzamelingenleer. Cantor's opvattingen over verzamelingen ondervonden veel oppositie. Cantor is zich bewust van de tegenstand:

> [...] ik ben mij ervan bewust dat ik mezelf met mijn onderneming plaats tegenover opvattingen over wiskundige oneindigheid die wijd zijn verbreid, en tegenover opvattingen over de aard van getallen die vaak worden verdedigd.

Hoe vruchtbaar het nieuwe perspectief op oneindigheid is blijkt uit de transfiniete getaltheorie, de grondslag voor het 'tellen' van oneindige verzamelingen. Een probleem waar Cantor mee bleef worstelen was de *continuum hypothese*, die inhoudt dat de graad van oneindigheid van de

reële getallen de graad van oneindigheid is die direct volgt op die van de natuurlijke getallen. Een aantal malen denkt Cantor een bewijs te pakken te hebben, maar nadere inspectie brengt steeds een foutje aan het licht.

Kurt Gödel (1906–1978)

Gödel is beroemd geworden met zijn *onvolledigheidsstellingen* uit 1931. Het bewijs laat zien dat in elk wiskundig axiomasysteem beweringen kunnen worden geformuleerd die binnen de axiomatiek van het systeem niet kunnen worden bewezen en niet kunnen worden weerlegd. Meer in het bijzonder: de consistentie van de axioma's valt niet te bewijzen. Uit Gödel's resultaten volgt ook direct dat het onmogelijk is computers zo te programmeren dat ze willekeurige wiskundige vragen kunnen beantwoorden.

In later werk liet Gödel zien dat de continuumhypothese (die Cantor had proberen te bewijzen) niet in strijd is met rest van de verzamelingenleer. Later bewees Paul Cohen dat noch de continuumhypothese, noch de negatie ervan, volgt uit de rest van de verzamelingenleer.

Dick de Bruijn (1918–. . .)

N.G.D. (Dick) de Bruijn is een Nederlands wiskundige. Hij promoveerde in 1943 op een proefschrift over algebraïsche getaltheorie. Na professoraten in Delft en Amsterdam werd hij in 1960 hoogleraar in Eindhoven. In 1967 startte hij in Eindhoven het *Automath* project. Hiermee werd hij een pionier op het gebied van met de computer verifiëren van wiskundige theorievorming. Dit werk leverde hem de Snellius medaille op in 1985.

De Bruijn was zijn tijd ver vooruit, maar inmiddels zijn er tal van programma's voor automatische verificatie van bewijzen. Bekende voorbeelden zijn *Coq* en *PVS*, allebei beschikbaar via internet. Zie `http://coq.inria.fr/` en `http://pvs.csl.sri.com/`.

Andrew Wiles (1953–. . .)

Andrew Wiles bewees in 1994 de laatste stelling van Fermat, zo genoemd omdat het de laatste stelling was waarvan Fermat claimde dat hij er een bewijs voor had, zonder dat bewijs te geven. De stelling zegt dat voor $n > 2$ de vergelijking $x^n + y^n = z^n$ geen positieve gehele oplossingen heeft.

Projecten

Modellen van hyperbolische meetkunde

In de tekst wordt het Klein-Beltrami model van hyperbolische meetkunde besproken. Een ander model van hyperbolische meetkunde is het Poincaré model. Zoek op het internet een beschrijving van het Poincaré model en probeer zo nauwkeurig mogelijk te omschrijven hoe het Klein-Beltrami model zich verhoudt tot het Poincaré model. Wat is de procedure om het Klein-Beltrami model in het Poincaré model om te zetten? Wat is de procedure om het Poincaré model in het Klein-Beltrami model om te zetten? Laat zien dat de omzetting van het ene model in het andere de Klein-Beltrami definitie van 'parallel aan' omzet in de Poincaré definitie van 'parallel aan', en omgekeerd. Net zo voor de definities van 'loodrecht op'.

Automatisch stellingen verifiëren

Zoek op het internet de software voor het bewijssysteem *Coq*. Installeer dit systeem op je computer. Gebruik de documentatie om ermee te leren werken. Formaliseer een aantal bewijzen uit dit boek, bij voorbeeld het bewijs van de irrationaliteit van $\sqrt{2}$.

Het Automath project

Zoek met behulp van internet en bibliotheek informatie over het *Automath* project van professor N.G. de Bruijn, en schrijf hierover een essay.

Een bewijs van Conway en Doyle doorgronden

Haal het artikel *Division by three* van John Conway en Peter Doyle [2] van het internet (`http://www.math.dartmouth.edu/~doyle/docs/three/three.pdf`). In dit artikel wordt bewezen dat als er een één-op-één correspondentie is tussen $3 \times A$ en $3 \times B$, dan is er ook een één-op-één correspondentie tussen A en B, hoe groot A en B ook zijn. Het bijzondere aan het bewijs is dat de gevraagde correspondentie ook echt wordt geconstrueerd. Dit artikel geeft je de kans om echte wiskundigen aan het werk te zien met het leveren van een interessant bewijs, waarbij je *en passant* nog allerlei wetenswaardigs leert over verzamelingen. De opdracht is om alle stappen in de bewijsvoering in dit artikel te doorgronden.

Meer projecten

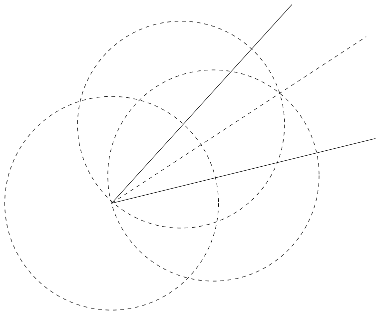
Meer projecten zijn te vinden op de internet pagina bij dit boek: `http://www.cwi.nl/~jve/qed/`.

Uitwerkingen van de Opdrachten

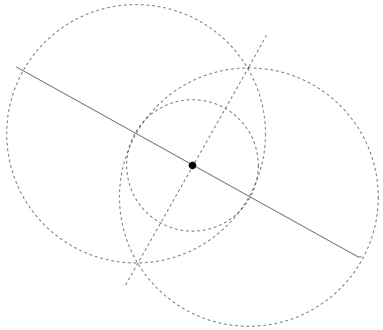
Hoofdstuk 1

Uitwerking van 1.1. In elk van de plaatjes zien we viermaal een rechthoekige driehoek. Noem de korte rechthoekszijde a, de lange rechthoekszijde b, en de schuine zijde c. Dan zien we dat de oppervlakte van het vierkant in het linkerplaatje wordt gegeven door: $(a+b)^2 = a^2 + 2ab + b^2$. Hierbij geeft $2ab$ dus de oppervlakte aan van de vier driehoeken samen. Het vierkant in het rechterplaatje is even groot, maar hier wordt de oppervlakte gegeven door $c^2 + 2ab$. Immers, $2ab$ is weer de oppervlakte van de vier driehoeken samen. Uit $a^2 + 2ab + b^2 = c^2 + 2ab$ volgt $a^2 + b^2 = c^2$, en dat moest worden aangetoond.

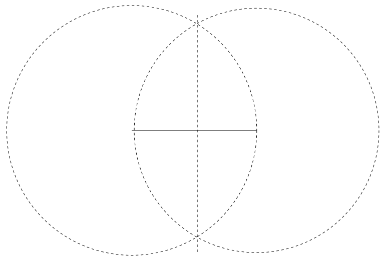
Uitwerking van 1.2.



Uitwerking van 1.3.



Uitwerking van 1.4.



Uitwerking van 1.5. Driehoek $\triangle BAD$ is gelijkbenig, dus $\angle DBA$ en $\angle ADB$ zijn gelijk, en $2\angle DBA + \angle BAD = 180°$. Driehoek $\triangle ACD$ is ook gelijkbenig, dus $\angle ACD$ en $\angle ADC$ zijn gelijk, en $2\angle ADC + \angle CAD = 180°$. Dus $2\angle BDC = 360° - (\angle BAC + \angle CAD) = 360° - 180° = 180°$, en $\angle BDC = 90°$.

Uitwerking van 1.6. Onze favoriete programmeertaal is Haskell (zie `www.haskell.org`). Een Haskell programma dat het gevraagde doet is het volgende. De ruimte ontbreekt om dit programma hier in detail uit te leggen; wie geïntrigeerd is zij verwezen naar de informatie over Haskell op het internet.

```
fact :: Integer -> Integer
fact 0 = 1
fact n = n * fact (n-1)

prime :: Integer -> Integer
prime n = until (\d -> rem q d == 0) succ (n+1)
  where q = fact n + 1

generate :: [(Integer,Integer,Integer)]
generate = map (\n -> (n, fact n + 1, prime n)) [1..]
```

Dit is het programma dat we gebruikt hebben om de tabel op bladzijde 14 te genereren. Verder dan die tabel komen we overigens niet ...

Hoofdstuk 2

Uitwerking van 2.1. Basisgeval: $2^5 = 32 > 5^2 = 25$.

Inductiestap: De inductiehypothese is $n \geq 5$ en $2^n > n^2$. We moeten op grond hiervan aantonen dat $2^{n+1} > (n+1)^2$. We hebben $2^{n+1} = 2 \cdot 2^n = 2^n + 2^n$ en $(n+1)^2 = n^2 + 2n + 1$. Omdat $2^n > n^2$ (inductie-hypothese) is het genoeg om te laten zien dat $n^2 > 2n + 1$, voor $n \geq 5$. Dat kan (voor wie dit niet direct gelooft) weer met inductie: $5^2 = 25 > 2 \cdot 5 + 1 = 11$ (basis), en: als $n^2 > 2n + 1$, dan $(n+1)^2 = n^2 + 2n + 1 \overset{ih}{>} (2n+1) + (2n+1) > 2(n+1) + 1 = 2n + 3$. De aanduiding $\overset{ih}{>}$ geeft aan waar de inductiehypothese is gebruikt in deze tweede inductie.

Uitwerking van 2.2. We moeten laten zien dat uit $a|b$ en $b|c$ volgt dat $a|c$. Neem dus aan dat $a|b$ en $b|c$. Om te laten zien dat $a|c$ moeten we een natuurlijk getal N vinden met de eigenschap dat $aN = c$. Uit $a|b$ weten we dat er een natuurlijk getal M is met $aM = b$, en uit $b|c$ weten we dat er een natuurlijk getal K is met $bK = c$. Als je nu aM invult voor b in $bK = c$ krijg je $aMK = c$. Neem $N = MK$, en je hebt aangetoond dat $a|c$.

Uitwerking van 2.3. Neem aan dat $n > 1$ terwijl $c = \mathrm{KD}(n)$ *geen* priemgetal is. Dit zou een tegenspraak moeten opleveren, en dat doet het ook. Immers, als c geen priemgetal is dan zijn er natuurlijke getallen a, b, elk groter dan 1, met $c = ab$. Maar dan is a zeker kleiner dan c, en $a|c$. Maar uit $a|c$ en $c|n$ volgt dat $a|n$ (opdracht 2.2). Dus is c niet de kleinste deler van n. De aanname dat $\mathrm{KD}(n)$ geen priemgetal is moet dus worden verworpen.

Uitwerking van 2.4. Neem aan dat n geen priemgetal is. Laat $b = \mathrm{KD}(n)$. Dan is er een a met $ba = n$. Dus $a|n$, maar omdat b de kleinste deler van n is geldt $b \leq a$. Maar dan is $b^2 \leq ba = n$, dat wil zeggen $(\mathrm{KD}(n))^2 \leq n$.

Uitwerking van 2.5. De som van de eerste n even getallen is gelijk aan $n(n+1)$.

Uitwerking van 2.6. Merk op dat de beweging die kever B maakt steeds haaks staat op de beweging van kever A. Het feit dat B beweegt ten opzichte van A is dus irrelevant: immers, de

beweging die B maakt brengt B niet dichterbij A en ook niet verder van A af. De afstand die A aflegt voordat hij B ontmoet is dus a (en net zo voor de andere kevertjes).

Uitwerking van 2.7. De snelheid waarmee de twee treinen elkaar naderen is 250 kilometer per uur, dus de botsing vindt plaats na precies een uur. In dat uur heeft de turbovlieg precies 200 kilometer afgelegd.

Uitwerking van 2.8. Het cruciale inzicht is dat bij elke stap het aantal witte steentjes *oneven* blijft. Immers, we beginnen met een oneven aantal witte steentjes. Stel dat we ergens middenin de procedure zitten, en er zit een oneven aantal witte steentjes in de vaas. Er zijn drie mogelijkheden:

1. Er worden twee witte steentjes getrokken. Er gaat nu een zwarte steen terug, en het aantal witte steentjes blijft oneven.

2. Er worden twee zwarte steentjes getrokken. Er gaat een zwarte steen terug. Het aantal witte steentjes verandert niet en blijft dus oneven.

3. Er wordt een zwart en een wit steentje getrokken. De witte gaat terug. Het aantal witte steentjes verandert niet en blijft dus oneven.

Als het laatste steentje zwart zou zijn, zou het aantal witte steentjes even zijn geworden (0 is even). Dat kan niet, dus het laatste steentje is wit.

Uitwerking van 2.9. $F_0 = 2^{2^0} + 1 = 3$, $F_1 = 2^{2^1} + 1 = 5$, $F_2 = 2^{2^2} + 1 = 17$, $F_3 = 2^{2^3} + 1 = 257$. $F_4 = 2^{2^4} + 1 = 65537$.

Uitwerking van 2.10. Het Haskell programma `map (\n -> 2^(2^n) + 1) [0..8]` geeft:

$$
\begin{array}{lcl}
F_0 & = & 3 \\
F_1 & = & 5 \\
F_2 & = & 17 \\
F_3 & = & 257 \\
F_4 & = & 65537 \\
F_5 & = & 4294967297 \\
F_6 & = & 18446744073709551617 \\
F_7 & = & 340282366920938463463374607431768211457 \\
F_8 & = & 115792089237316195423570985008687907853269984665640564039457584007913129639937
\end{array}
$$

Dit loopt verschrikkelijk snel op. Ontbinden in factoren is met simpele programma's vrijwel onbegonnen werk. Verder dan $18446744073709551617 = 274177 \cdot 67280421310721$ komen we niet.

Uitwerking van 2.11.

$$
\begin{array}{lll}
 & a_0 = 90 & b_0 = 42 \\
a_0 > b_0 & a_1 = 48 & b_1 = 42 \\
a_1 > b_1 & a_2 = 6 & b_2 = 42 \\
a_2 < b_2 & a_3 = 6 & b_3 = 36 \\
a_3 < b_3 & a_4 = 6 & b_4 = 30 \\
a_4 < b_4 & a_5 = 6 & b_5 = 24 \\
a_5 < b_5 & a_6 = 6 & b_6 = 18 \\
a_6 < b_6 & a_7 = 6 & b_7 = 12 \\
a_7 < b_7 & a_8 = 6 & b_8 = 6 \\
a_8 = b_8 = 6 & &
\end{array}
$$

$$
\begin{array}{lll}
 & a_0 = 90 & b_0 = 43 \\
a_0 > b_0 & a_1 = 47 & b_1 = 43 \\
a_1 > b_1 & a_2 = 4 & b_2 = 43 \\
a_2 < b_2 & a_3 = 4 & b_3 = 39 \\
a_3 < b_3 & a_4 = 4 & b_4 = 35 \\
a_4 < b_4 & a_5 = 4 & b_5 = 31 \\
a_5 < b_5 & a_6 = 4 & b_6 = 27 \\
a_6 < b_6 & a_7 = 4 & b_7 = 23 \\
a_7 < b_7 & a_8 = 4 & b_8 = 19 \\
a_8 < b_8 & a_9 = 4 & b_9 = 15 \\
a_9 < b_9 & a_{10} = 4 & b_{10} = 11 \\
a_{10} < b_{10} & a_{11} = 4 & b_{11} = 7 \\
a_{11} < b_{11} & a_{12} = 4 & b_{12} = 3 \\
a_{12} > b_{12} & a_{13} = 1 & b_{13} = 3 \\
a_{13} < b_{13} & a_{14} = 1 & b_{14} = 2 \\
a_{14} < b_{14} & a_{15} = 1 & b_{15} = 1 \\
a_{15} = b_{15} = 1 & &
\end{array}
$$

Uitwerking van 2.12. Stel $a > b$. Als d deler is van a en van b dan zijn er m, n met $dm = a$ en $dn = b$. Dus is $a - b = d(m - n)$, dat wil zeggen: d deelt $a - b$. Als d deler is van $a - b$ en van b dan zijn er m, n met $dm = a - b$ en $dn = b$. Dus is $a = (a - b) + b = dm + dn = d(m + n)$, dat wil zeggen: d deelt a. De redenering voor het geval $a > b$ gaat evenzo.

Uitwerking van 2.13. Stel dat er natuurlijke getallen p en q zijn, met $q \neq 0$, zodanig dat $\left(\frac{p}{q}\right)^2 = 3$. Neem ook aan dat p en q geen factoren gemeen hebben. Dan is $\frac{p^2}{q^2} = 3$, dus $p^2 = 3q^2$. Hieruit volgt dat p een factor 3 moet hebben, want als dat niet zo is dan is 3 ook geen factor van p^2. Dus $p = 3a$ voor zekere $a \in \mathbb{N}$. Hieruit volgt: $p^2 = (3a)^2 = 9a^2 = 3q^2$, en we krijgen nu dus ook dat $q^2 = 3a^2$. Daaruit volgt weer dat ook q een factor 3 heeft. Hiermee zijn we in tegenspraak gekomen met de aanname dat p en q geen factoren gemeen hebben.

Uitwerking van 2.14. Stel dat $\sqrt{2}+\sqrt{3}$ een breuk is, zeg $\frac{p}{q}$. We weten dat $(\sqrt{2}+\sqrt{3})(\sqrt{2}-\sqrt{3}) = -1$, dus $\sqrt{2} - \sqrt{3} = -\frac{q}{p}$. Hieruit volgt:

$$2\sqrt{2} = (\sqrt{2} + \sqrt{3}) + (\sqrt{2} - \sqrt{3}) = \frac{p}{q} - \frac{q}{p} = \frac{p^2 - q^2}{pq}.$$

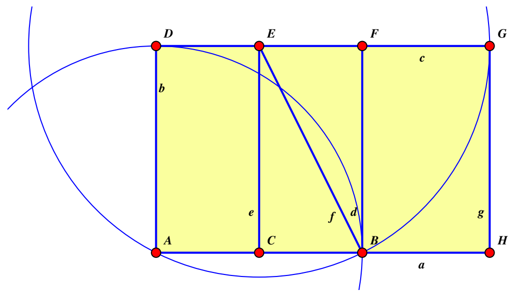
Dit brengt ons in tegenspraak met het feit dat $\sqrt{2}$ geen breuk is. Dus $\sqrt{2} + \sqrt{3}$ is ook geen breuk.

Uitwerking van 2.15. We moeten laten zien dat als p priem is, dan is $\sqrt{p}$ geen breuk. Neem dus aan dat p priem is en dat $\sqrt{p}$ wel een breuk is. Dan zijn er dus $n, m \in \mathbb{N}$ met $\left(\frac{n}{m}\right)^2 = p$. We nemen weer aan dat n en m geen factoren gemeen hebben. Dan is $\frac{n^2}{m^2} = p$, en dus $n^2 = pm^2$. Uit het feit dat p priem is volgt nu dat n een factor p heeft, want kwadrateren introduceert geen nieuwe priemfactoren. Maar dan is er een $a \in \mathbb{N}$ met $n = pa$. Hieruit volgt dat $n^2 = p^2a^2 = pm^2$, en dus $m^2 = pa^2$. Er volgt dat ook m een factor p heeft, en dit geeft een tegenspraak met de aanname dat n en m geen factoren gemeen hebben.

Uitwerking van 2.16. We moeten laten zien: als $n \in \mathbb{N}$ en $\sqrt{n} \notin \mathbb{N}$, dan is $\sqrt{n}$ geen breuk. Neem $n \in \mathbb{N}$ met $\sqrt{n} \notin \mathbb{N}$, en veronderstel dat $\sqrt{n}$ een breuk is. Dan zijn er $p, q \in \mathbb{N}$ met $q \neq 0$ en $\sqrt{n} = \frac{p}{q}$. Weer nemen we aan dat p en q geen factoren gemeen hebben. Uit dit laatste volgt dat ook p^2 en q^2 geen factoren gemeen hebben (kwadrateren introduceert geen nieuwe priemfactoren). Aan de andere kant krijgen we uit $\sqrt{n} = \frac{p}{q}$ dat $n = \frac{p^2}{q^2}$, dus q^2 is een deler van p^2, en een tegenspraak.

Opmerking: als je goed naar opdrachten 2.15 en 2.16 kijkt zie je dat 2.15 een speciaal geval is van 2.16. Een efficiënte bewijsmethode is dus: eerst 2.16 bewijzen, en vervolgens 2.15 aanpakken door op te merken: als p priem is dan is $\sqrt{p}$ zeker geen natuurlijk getal, dus volgt uit 2.16 dat $\sqrt{p}$ geen breuk is.

Uitwerking van 2.17. Stel dat ${}^{10}\log 2 = p/q$ voor positieve gehele getallen p en q. Dan geldt wegens de betrekking $L = {}^{b}\log a \Leftrightarrow b^L = a$ dat $10^{p/q} = 2$. Beide zijden verheffen tot de q-de macht geeft $10^p = 2^q$. Dit is onmogelijk, want er valt gemakkelijk in te zien dat alle positieve machten van 10 als laatste cijfer een 0 hebben, terwijl alle positieve machten van 2 als laatste cijfer een 2, 4, 8 of 6 hebben.



Figuur 6.1: De Gulden Snede.

Uitwerking van 2.18. Stel de zijde van het vierkant $ABFD$ in Figuur 6.1 gelijk aan 2. Dan is $|EF| = 1$ en $|BF| = 2$, dus met de stelling van Pythagoras: $|EB| = \sqrt{5}$ en $|DG| = |DE|+|EG| =$

$|DE| + |EB| = 1 + \sqrt{5}$.

Stel nu dat $\frac{1+\sqrt{5}}{2}$ een breuk is, zeg $\frac{1+\sqrt{5}}{2} = p/q$. Dan $\sqrt{5} = \frac{2p-q}{q}$, en tegenspraak met de uitkomst van opdracht 2.15 (of met die van opdracht 2.16).

Uitwerking van 2.19. Beschouw de regelmatige vijfhoek $ABCDE$ van Figuur 2.3 op bladzijde 33. In die vijfhoek is AB een zijde, en AC en AD zijn diagonalen. Vouw de driehoek ABC naar binnen langs diagonaal AC. Daarbij komt punt B op de diagonaal AD terecht, op punt B'. De driehoeken $\triangle ACD$ en $\triangle CDB'$ zijn congruent. Stel de lengte van de diagonaal AD gelijk aan x en de lengte van de zijde AB gelijk aan 1. Dan is $|DB'| = |AD| - |AB'| = |AD| - |AB| = x - 1$. Wegens gelijkvormigheid van $\triangle ACD$ en $\triangle CDB'$ geldt dus: $x : 1 = 1 : (x-1)$. Dus is $x = \frac{1}{1-x}$, dat wil zeggen $x(x-1) = 1$, ofwel $x^2 - x - 1 = 0$. Oplossen van deze vergelijking met behulp van de formule $x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$ geeft $x = \frac{1\pm\sqrt{5}}{2}$. Combinatie met het feit dat x positief is geeft $x = \frac{1+\sqrt{5}}{2}$. Inderdaad de gulden snede.

Uitwerking van 2.20. Als $\sqrt[3]{2} = p/q$, dan is $2q^3 = p^3$. In de representatie van p^3 als product van priemfactoren zullen alle priemfactoren voorkomen in veelvouden van 3, want de derde macht van een getal is gelijk aan het product van de derde machten van de priemfactoren van dat getal. In de representatie van $2q^3$ komt de factor 2 echter $3n+1$ maal voor, voor zekere n. Omdat volgens Stelling 2.4 de representatie uniek is is dit onmogelijk.

Uitwerking van 2.21. Laat $A = \{4n + 3 \mid n \in \mathbb{N}\}$, en neem aan dat A slechts eindig veel priemgetallen bevat. Dan is er een eindige verzameling $\{p_1, \ldots, p_n\}$ van alle priemgetallen in A. Beschouw nu het getal $Q = 4p_1 \cdots p_k - 1 = 4(p_1 \cdots p_k - 1) + 3$.

Als Q priem is, dan hebben we een tegenspraak met de aanname, en klaar. Als Q niet priem is, dan heeft Q een priemfactor P die verschilt van elke p_i. Immers, elke p_i deelt Q met rest -1. Als P de vorm $4n+3$ heeft zijn we klaar, want dan is P immers een priemgetal in A dat niet in de oorspronkelijke lijst $p_1, \ldots, p_n$ zit. Neem dus aan dat P van de vorm $4n+1$ is (meer mogelijkheden zijn er niet). Nu maken we gebruik van het feit dat $(4a+1)(4b+1)$ van de vorm $(4c+1)$ is. Vanwege dit feit, dat je kunt inzien de vermenigvuldiging $(4a+1)(4b+1)$ uit te voeren, is $\frac{Q}{P}$ van de vorm $4n+3$. Ook moet $\frac{Q}{P}$ een priemfactor q_1 hebben. Na een eindig aantal stappen levert dit een priemfactor q_i op die van de vorm $4n+3$ is, met $q_i \neq p_1, \ldots, p_k$, en dat geeft ons de gezochte tegenspraak.

Uitwerking van 2.22. Noem het nieuwe papiertje *nieuw*, en de twee mogelijkheden voor het oude papiertje oud_{wit} en oud_{zwart}. Er zijn nu vier mogelijkheden:

1. *nieuw* wordt getrokken, en vervolgens oud_{wit}.
2. *nieuw* wordt getrokken, en vervolgens oud_{zwart}.
3. oud_{wit} wordt getrokken, en vervolgens *nieuw*.
4. oud_{zwart} wordt getrokken, en vervolgens *nieuw*.

De laatste mogelijkheid doet zich niet voor: het is immers gegeven dat het eerste papiertje dat getrokken wordt wit is. De andere drie mogelijkheden zijn elk even waarschijnlijk. De kans dat het tweede papiertje ook wit is is dus $\frac{2}{3}$.

Uitwerking van 2.23. In een gezin van twee kinderen met minstens een jongen zijn er drie mogelijkheden:

1. de oudste is een jongen, de jongste een jongen;
2. de oudste een jongen, de jongste een meisje;
3. de oudste een meisje, de jongste een jongen.

Alle drie deze mogelijkheden zijn even waarschijnlijk. De kans op twee jongens is dus $\frac{1}{3}$. In een gezin van twee kinderen met de oudste een meisje zijn er maar twee mogelijkheden:

1. de jongste is een meisje;
2. de jongste is een jongen.

Weer: allebei even waarschijnlijk. De kans op twee meisjes is dus $\frac{1}{2}$.

Uitwerking van 2.24. Op het moment dat je je oorspronkelijke keus maakt is elk van de drie deuren even waarschijnlijk. Je kans om te winnen met de keuze van deur 1 is dus $\frac{1}{3}$, en de kans dat de cabrio achter deur 2 of deur 3 staat is $\frac{2}{3}$. Als de quizmaster verklapt dat de cabrio niet achter deur 2 staat is de waarschijnlijkheid dat hij achter deur 3 staat dus $\frac{2}{3}$. Door je keuze te herzien kun je je kans om te winnen dus verdubbelen.

Zoals altijd zijn er meerdere wegen naar het juiste inzicht. We bekijken de zaak even algemeen, en noemen de deuren A, B, C. Je kiest deur A. Er zijn nu drie mogelijkheden:

1. De cabrio staat achter deur A. De quizmaster doet een van de andere deuren open. Als je je keuze herziet verlies je.
2. De cabrio staat achter deur B. De quizmaster doet deur C open. Als je je keuze herziet win je.
3. De cabrio staat achter deur C. De quizmaster doet deur B open. Als je je keuze herziet win je.

Keuze herzien geeft dus in een van de drie mogelijke gevallen verlies en in de twee andere winst. Het is duidelijk dat je je keuze moet herzien.

Uitwerking van 2.25. In het eerste voorbeeld in de stap waar gedeeld wordt door $a - a$, want delen door 0 is niet toegestaan. In het tweede voorbeeld, in de stap waar gedeeld wordt door $a - b$. Omdat $a = b$, is $a - b$ gelijk aan 0, en delen door 0 is niet toegestaan.

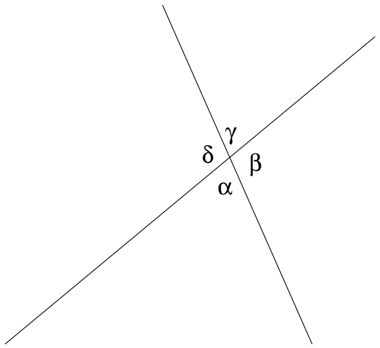
Uitwerking van 2.26. Redeneren over de gelijkheid van sommen van oneindige reeksen is alleen zinvol wanneer die reeksen convergeren. Welnu, de reeks $1 - 1 + 1 - 1 + 1 - 1 + 1 - 1 + \cdots$ convergeert niet: de waarde slaat steeds om van 1 naar 0 en vice versa.

Uitwerking van 2.27. De fout zit in "Neem nu $r \in A - \{p, q\}$." Dit kan alleen als $A - \{p, q\}$ niet leeg is. Maar stel nu dat A twee elementen bevat, en p en q zijn twee verschillende elementen van A. Dan is $A - \{p, q\} = \emptyset$.

Hoofdstuk 3

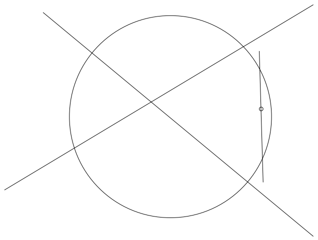
Uitwerking van 3.1. We hanteren het *Van Dale Basiswoordenboek van de Nederlandse Taal*, door Monique Huygen en Marja Verburg (1996). Dit woordenboek omschrijft *verzameling* als "groep van dingen die je bij elkaar hebt gebracht en die samen een geheel vormen, ⇒ collectie." *Groep* wordt omschreven als "aantal mensen, dieren of dingen die bij elkaar horen", *collectie* als "verzameling, vaak van waardevolle of interessante dingen." Hier hebben we al een cirkel, en dat is heus niet omdat het *Van Dale Basiswoordenboek* een woordenboek is voor kinderen.

Uitwerking van 3.2.



Uit $\alpha = 180° - \beta$ en $\beta = 180° - \gamma$ volgt $\alpha = \gamma$. Uit $\alpha = \gamma$ volgt $180° - \alpha = 180° - \gamma$, dat wil zeggen $\beta = \delta$. Het enige postulaat dat we nodig hebben is postulaat IV: alle rechte hoeken zijn gelijk. Hieruit volgt meteen dat alle gestrekte hoeken gelijk zijn.

Uitwerking van 3.3.



Uitwerking van 3.4. Laat een Klein-Beltrami model gegeven zijn met een lijn l en een punt P. Als l een middellijn is van de schijf, d.w.z., een lijn die door het middelpunt van de schijf gaat, dan is de Euclidische loodlijn door P op l de gevraagde hyperbolische loodlijn. Dit volgt uit de eerste clausule in de definitie van 'loodrecht'. Als l geen middellijn is van de schijf dan heeft l een pool M. De lijn PM is nu de gevraagde loodlijn. Dit volgt uit de tweede clausule in de definitie van 'loodrecht'.

Uitwerking van 3.5. In de Riemann meetkunde worden tegenover elkaar liggende punten met elkaar geïdentificieerd. Dus de Noord- en de Zuidpool van de bol zijn in feite hetzelfde punt. Door dit ene punt gaan oneindig veel lijnen (grootcirkels), maar zodra je een punt neemt dat *niet* samenvalt met een van de polen gaat er door dat punt en de pool precies één grootcirkel. Precies als bij Euclidische meetkunde, dus.

Uitwerking van 3.6. De afstand tussen twee punten is in de lengte van de kortste boog langs de grootcirkel die de twee punten met elkaar verbindt. Precies zoals je de afstand tussen Amsterdam en Moskou zou meten, dus.

Uitwerking van 3.7. De som van de hoeken van een driehoek is in de Riemann meetkunde groter dan twee rechte hoeken. Kijk maar naar de driehoek op het aardoppervlak die gevormd wordt door de Greenwich meridiaan 0°, de meridiaan 90°, en de Evenaar, met de Noordpool als tophoek. Elk van de drie hoeken in deze driehoek is recht, dus de som van de hoeken van de driehoek is gelijk aan *drie* rechte hoeken.

Uitwerking van 3.8. De hypothese dat de kosmische ruimte Euclidisch is laat zich door meten niet verifiëren (er is immers altijd een meetfout), maar hoogstens falsifiëren. Maar dat wil zeggen dat de hypothese dat de kosmische ruimte *niet* Euclidisch is zich door meten niet laat falsifiëren, maar hoogstens verifiëren. Het formele verschil tussen de twee hypothesen 'de kosmische ruimte is Euclidisch' en 'de kosmische ruimte is hyperbolisch' zit hem in het feit dat de eerste hypothese geen existentiebewering doet maar de tweede juist wel: "er is een driehoek te vinden met een som van de hoeken kleiner dan 180°."

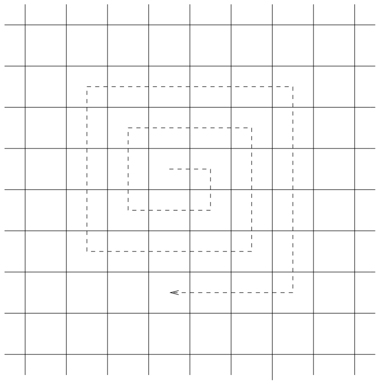
Uitwerking van 3.9. Als we in het Euclidische vocabulair praten over het Euclidische vlak (of over het gedeelte ervan dat binnen de Klein-Beltrami schijf ligt) dan zijn *punten* inderdaad gewoon punten en *cirkels* gewoon cirkels. Maar we kunnen ook in het hyperbolische vocabulair praten over wat binnen de Klein-Beltrami schijf van het Euclidische vlak ligt. Dan zijn **punten** de punten die binnen de schijf liggen, en **cirkels** de verzamelingen van **punten** die allemaal dezelfde **afstand** hebben tot een gegeven **punt**. Omdat **afstand** niet hetzelfde betekent als *afstand* zijn de definities van **cirkel** en *cirkel* dus verschillend.

Hoofdstuk 4

Uitwerking van 4.1. 'kwadrateren' op de reële getallen is geen injectie, want de kwadraten van (bij voorbeeld) 2 en -2 zijn identiek. Het is ook geen surjectie, want er zitten geen negatieve getallen in het beeld van de functie. Omdat het geen injectie of surjectie is is het dus zeker ook geen bijectie.

Uitwerking van 4.2. 'Vermenigvuldigen met 2' op de natuurlijke getallen is een injectie, want uit $m \neq n$ volgt dat $2m \neq 2n$. Het is geen surjectie, want oneven getallen komen niet in het beeld van de functie voor. Omdat het geen surjectie is is het zeker ook geen bijectie.

Uitwerking van 4.3. 'Vermenigvuldigen met 2' op de reëele getallen is een injectie, want uit $x \neq y$ volgt dat $2x \neq 2y$. Het is ook een surjectie, want elk reëel getal y kan worden geschreven als $2x$, voor $x = \frac{y}{2}$. Omdat de functie zowel een injectie als een surjectie is is het een bijectie.



Figuur 6.2: Aftellen van de velden van een oneindig schaakbord.

Uitwerking van 4.4. Een oneindig schaakbord kan worden afgeteld op de manier van Figuur 6.2.

Uitwerking van 4.5. De breuk t/n ligt op plaats t op de diagonaal die volgt op de driehoek met hoekpunten $1/n$, $1/(t+n-2)$, en $(t+n-2)/1$. Het rangnummer is dus $\frac{(t+n-2)(t+n-1)}{2} + t$. Dit wil zeggen dat de formule $f(t,n) = \frac{(t+n-2)(t+n-1)}{2} + t$ voldoet.

Je kunt de aftelling van de paren van positieve natuurlijke getallen als volgt programmeren (weer in onze favoriete taal Haskell):

```
pnatpairs = [(x,z-x) | z <- [1..], x <- [1..(z-1)]]
```

Dit geeft:

```
Main> take 12 pnatpairs
[(1,1),(1,2),(2,1),(1,3),(2,2),(3,1),(1,4),(2,3),(3,2),(4,1),(1,5),(2,4)]
```

De zojuist gegeven functie heeft de volgende implementatie:

```
ppair (t,n) = (t + n - 2) * (t + n - 1) `div` 2 + t
```


Samen geeft dit:

```
Main> take 12 (map ppair pnatpairs)
[1,2,3,4,5,6,7,8,9,10,11,12]
```

Uitwerking van 4.6. Neem aan dat de kamers van het Hilbert Hotel genummerd zijn als $0, 1, 2, \ldots$. Laat de gast van kamer 0 verhuizen naar kamer 1, die van kamer 1 naar kamer 2, en in het algemeen die van kamer n naar kamer $n+1$. Kamer 0 komt nu vrij voor de nieuwe gast.

Uitwerking van 4.7. Laat de gast van de kamer met nummer n verhuizen naar die met nummer $2n$. Dan zitten alle oude gasten in een kamer met een even nummer. De kamers met de oneven nummers komen nu vrij voor de inzittenden van de Hilbert bus.

Uitwerking van 4.8. Laat f een aftelling zijn van de hotelgasten, en h_0, h_1, h_2, $\ldots$ aftellingen van de inzittenden van de verschillende Hilbert bussen. Dan kan dit totaal worden afgeteld met behulp van Cantor's aftelprocedure voor de breuken:

$$
\begin{array}{ccccccccccccc}
f(0) & & f(1) & & f(2) & & f(3) & & f(4) & & f(5) & \cdots \\
 & \swarrow & & \swarrow & & \swarrow & & \swarrow & & \swarrow & & \\
h_0(0) & & h_0(1) & & h_0(2) & & h_0(3) & & h_0(4) & & h_0(5) & \cdots \\
 & \swarrow & & \swarrow & & \swarrow & & \swarrow & & & & \\
h_1(0) & & h_1(1) & & h_1(2) & & h_1(3) & & h_1(4) & & h_1(5) & \cdots \\
 & \swarrow & & \swarrow & & \swarrow & & & & & & \\
h_2(0) & & h_2(1) & & h_2(2) & & h_2(3) & & h_2(4) & & h_2(5) & \cdots \\
 & \swarrow & & \swarrow & & & & & & & & \\
h_3(0) & & h_3(1) & & h_3(2) & & h_3(3) & & h_3(4) & & h_3(5) & \cdots \\
 & \swarrow & & & & & & & & & & \\
h_4(0) & & h_4(1) & & h_4(2) & & h_4(3) & & h_4(4) & & h_4(5) & \cdots \\
\text{etc} & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots &
\end{array}
$$

Uitwerking van 4.9. Elke niet-lege eindige deelverzameling van $\mathbb{N}$ bevat een grootste getal n. Het is duidelijk dat er eindig veel deelverzamelingen van $\mathbb{N}$ zijn waarin n het grootste getal is; om precies te zijn zijn het er 2^n. We kunnen dus als volgt aftellen: eerst $\emptyset$, dan de ene deelverzameling met 0 als grootste element, dan de twee deelverzamelingen met 1 als grootste element, dan de vier deelverzamelingen met 2 als grootste element, enzovoorts.

Uitwerking van 4.10. Een getal n codeert een verzameling X_n als volgt. Schrijf de binaire representatie van n op. Dan definiëren we $m \in X_n$ dan en slechts dan als op de $n+1$-e plaats tellende van rechts naar links in de binaire representatie van n een 1 staat. Dit geeft aan elke eindige deelverzameling van $\mathbb{N}$ een unieke code. Immers, de code voor $\emptyset$ is 0 en de code voor $\{a_1, \ldots, a_n\}$ is $2^{a_1} + \cdots + 2^{a_n}$.

Uitwerking van 4.11.

- Welke punten zitten in een eindige lus? Alleen het punt 0, want we hebben $0 \xrightarrow{f} 0 \xrightarrow{g} 0$. Dit geeft: $h(0) = 0$.

- Welke punten zitten in een naar beide zijden oneindige rij? Geen.
- Welke punten zitten in een oneindige reeks die met een punt in $[0,1]$ begint? Het enige beginpunt is 1, want de g voorganger van 1 is 1, en dat punt zit niet in het domein van g. De oneindige reeks bestaat uit de punten in $X = \{\frac{1}{2^n} \mid n \in \mathbb{N}\}$. Het voorschrift luidt: $h(x) = \frac{1}{2}x$ voor $x \in X$.
- Welke punten zitten in een oneindige reeks die met een punt in $[0,1)$ begint? De beginpunten zitten in het open interval $(\frac{1}{2}, 1)$. Immers, de verzameling f-voorgangers van dat interval wordt gevormd door het open interval $(1,2)$, en dat is disjunct van $[0,1]$. De verzameling van alle punten in een oneindige reeks die met een g-stap begint wordt gevormd door $Y = \bigcup\{(\frac{1}{2\cdot 2^n}, \frac{1}{2^n}) \mid n \in \mathbb{N}\}$. Dit zijn precies alle positieve getallen ≤ 1 die *niet* van de vorm $\frac{1}{2^n}$ zijn, dat wil zeggen: $Y = (0,1] - X$. Het voorschrift luidt: $h(x) = x$ voor $x \in Y$.

De h die we zo krijgen kan gedefinieerd worden als: $h(x) = \frac{1}{2}x$ voor x van de vorm $\frac{1}{2^n}$, $h(x) = x$ anders. Het valt gemakkelijk in te zien dat h een bijectie is.

Hoofdstuk 5

Uitwerking van 5.1.

Van (1) naar (2).
Stel $A \subseteq B$, dat wil zeggen: elk element van A is element van B.
Te bewijzen: $A \cap B = A$.
Bewijs: De elementen van $A \cap B$ zijn de elementen die zowel in A als in B zitten.
Omdat elk element van A in B zit zijn dit precies de elementen in A.

Van (2) naar (3).
Stel $A \cap B = A$.
Te bewijzen: $A \cup B = B$.
Bewijs: De elementen van $A \cup B$ zijn de elementen die in A of in B zitten.
Volgens het gegeven zitten de elementen van A in A en in B.
Dus de elementen van $A \cup B$ zijn zijn de elementen die in (A en B) of in B zitten.
Dit zijn precies de elementen van B.

Van (3) naar (1).
Stel $A \cup B = B$.
Te bewijzen: $A \subseteq B$.
Bewijs: Neem een willekeurig element x van A. Dan $x \in A \cup B$.
Dus volgens gegeven $x \in B$.
Dus $A \subseteq B$.

Uitwerking van 5.2.
Van (1) naar (2).
Stel n is deelbaar door 3.
Te bewijzen: $3n$ is deelbaar door 9.

Bewijs: Uit de aanname volgt dat er een $m \in \mathbb{N}$ is met $n = 3m$.
Dus $3n = 3(3m) = 9m$, d.w.z., $3n$ is deelbaar door 9.

Van (2) naar (3).
Stel $3n$ is deelbaar door 9.
Te bewijzen: $n + 3$ is deelbaar door 3.
Bewijs: Uit de aanname: er is een $k \in \mathbb{N}$ met $3n = 9k$.
Dus $n = 3k$, en $n + 3 = 3k + 3 = 3(k + 1)$, d.w.z., $n + 3$ is deelbaar door 3.

Van (3) naar (1).
Stel $n + 3$ is deelbaar door 3.
Te bewijzen: n is deelbaar door 3.
Bewijs: Uit de aanname: er is een $k \in \mathbb{N}$ met $n + 3 = 3k$.
Dus $n = 3k - 3 = 3(k - 1)$, d.w.z., n is een drievoud.

Uitwerking van 5.3.
Er zijn drie mogelijkheden: (1) n is deelbaar door 3. Dan $n(n+1)(n+2)$ zeker ook. (2) $n+1$ is deelbaar door 3. Dan $n(n+1)(n+2)$ zeker ook. (3) $n+2$ is deelbaar door 3. Dan $n(n+1)(n+2)$ zeker ook.

Uitwerking van 5.4. De bewering is onwaar. $A = \{1,2\}$ en $B = \{2,3\}$ levert een tegenvoorbeeld. We hebben dan:

$$\wp(A \cup B) = \wp(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.$$

$$\begin{aligned}
\wp A \cup \wp B &= \wp\{1,2\} \cup \wp\{2,3\}) \\
&= \{\emptyset, \{1\}, \{2\}, \{1,2\}\} \cup \{\emptyset, \{2\}, \{3\}, \{2,3\}\} \\
&= \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}\}.
\end{aligned}$$

Literatuur

Als je van wiskunde houdt heb je geluk, want dan gaan er werelden voor je open die voor anderen gesloten blijven. Die werelden worden beschreven in prachtige boeken, meestal in het Engels, maar je zult zien dat je daar snel genoeg aan bent gewend.

De axiomatische methode staat centraal in [10], een zeer leesbaar boekje over wiskunde dat niet meer veronderstelt dan wat je in de brugklas hebt geleerd. Dit is een geslaagde poging om aan een algemeen publiek duidelijk te maken hoe wiskundigen denken, vertaald in het Nederlands.

Een leuk boek over muziektheorie en wiskunde (blz. 12), en nog in het Nederlands ook, is [5]. Als je in muziektheorie bent geïnteresseerd zou je ook kunnen beginnen met het veel beknoptere [6], van dezelfde auteur. Allerlei wetenswaardigs over grootste gemene delers, kleinste gemene veelvouden en priemgetallen vind je in [8], ook in de Zebra reeks (die hele reeks is trouwens zeer aanbevolen).

Een mooie beschrijving van de ontwikkeling van Euclidische en niet-Euclidische meetkunde is te vinden in [11]. Een Nederlandse bewerking van Euclides' Elementen zul je misschien nog in een bibliotheek kunnen vinden: [7].

Een klassiek en goed geschreven overzicht van ideeën en methoden van de wiskunde, en een boek dat iedereen met belangstelling voor wiskunde zou moeten kopen en lezen is Courant en Robbins, *What is Mathematics* [4]. Hier is wat Albert Einstein ervan zegt:

> Een heldere uiteenzetting over de fundamentele begrippen en methoden die het hele terrein van de wiskunde beslaat. Dit is een gemakkelijk te volgen inleiding voor de leek, maar ook geschikt om wie wiskunde studeert een algemeen beeld te geven van de grondprincipes en methoden.

Een prachtig boek over zuivere wiskunde is *The Book of Numbers* [3]. In dit boek staat het begrip 'getal' centraal. Twee top-wiskundigen leggen uit hoe rijk dit begrip is, zonder specialistische voorkennis te veronderstellen. Getallen om te tellen, nul, breuken, negatieve getallen, kwadratische irrationalen, algebraische getallen, transcendente getallen, infinitesimalen en transfiniete getallen, surreële getallen, complexe getallen, quaternionen, octonionen passeren de revue. Alles wordt verduidelijkt met schitterende illustraties. Een onuitputtelijk boek.

Als je wilt weten hoe wiskunde er voor wiskundigen uitziet, en wat het zo leuk maakt, dan moet je *The Pleasures of Counting* van T.W. Körner [13] lezen. Dit boek is bedoeld voor iedereen met belangstelling voor wiskunde en toepassingen van wiskundig denken. Hoewel de auteur

beweert dat hij zijn boek geschreven heeft voor getalenteerde lezers en lezeressen van 14 jaar en ouder moet je niet verwachten dat je elke passage meteen zult begrijpen. Wanneer echte wiskundigen een goed wiskundeboek lezen is dat trouwens ook zo. Als ze alles zouden begrijpen zouden ze het boek verveeld terzijde schuiven: te gemakkelijk. Mooie achtergrondverhalen over de rol die wiskunde speelde bij het bestrijden van cholera, bij het beschermen van konvooien tegen aanvallen van duikboten, bij het ontwerpen van ankers voor zeiljachten, en nog veel meer.

De Hongaarse wiskundige Paul Erdós (1913–1996) sprak graag over Het Boek, waarin God de volmaakte bewijzen voor wiskunde stellingen bijhoudt. Volgens Erdós hoef je niet in God te geloven, maar als wiskundige moet je op zijn minst geloven in Het Boek. Een benadering van Het Boek is te vinden in [1]. Vol briljante ideeën, heldere inzichten en prachtige observaties.

Het programma *Cinderella* dat gebruikt is om de meetkunde applets bij dit boek te produceren wordt gedocumenteerd in [16].

Bibliografie

[1] M. Aigner and G.M. Ziegler. *Proofs from THE BOOK*. Springer, 1998.

[2] J. Conway and P. Doyle. Division by three. `http://www.math.dartmouth.edu/~doyle/docs/three/three.pdf`, 1994.

[3] J.H. Conway and R.K. Guy. *The Book of Numbers*. Springer, 1996.

[4] R. Courant and H. Robbins (revised by I. Stewart). *What is Mathematics? An Elementary Approach to Ideas and Methods (Second Edition)*. Oxford University Press, Oxford, 1996.

[5] Jan van de Craats. *De fis van Euler*. Aramith, 1989.

[6] Jan van de Craats. *De juiste toon*. Zebra-reeks. Epsilon uitgaven, 2003.

[7] E.J. Dijksterhuis. *De elementen van Euclides*. Noordhoff, Groningen, 1929–1930.

[8] R. Jeurissen en L. van den Broek. *Spelen met gehelen*. Zebra-reeks. Epsilon uitgaven, 2002.

[9] Euclid. *The Thirteen Books of the Elements, with Introduction and Commentary by Sir Thomas L. Heath*. Dover, 1956.

[10] T. Gowers. *De kortste introductie wiskunde*. Spectrum, 2002.

[11] M.J. Greenberg. *Euclidean and Non-Euclidean Geometries*. W.H. Freeman, 1974. Reprinted in 1996.

[12] G.H. Hardy. *A mathematician's apology*. Cambridge University Press, 1940.

[13] T.W. Körner. *The Pleasures of Counting*. Cambridge University Press, 1996.

[14] M. Laczkovich. *Conjecture and Proof*. The Mathematical Association of America, 2001.

[15] G. Polya. *How to Solve It. A New Aspect of Mathematical Method*. Princeton University Press, Princeton, 1957.

[16] J. Richter-Gebert and U.H. Kortenkamp. *The Interactive Geometry Software Cinderella*. Springer, 1999. Internet support on `www.cinderella.de`.

[17] R.J. Trudeau. *The Non-Euclidean Revolution*. Birkhauser Boston, 1995. Reprint of 1987 edition.

Flaptekst

De notie *bewijs* vormt het hart van de exacte wetenschappen. De ontdekking van de methode om een onderwerp te presenteren in termen van axioma's, definities en bewijzen is een van de grote uitvindingen van de Mensheid. Het beroemdste voorbeeld van deze axiomatische methode is de systematische presentatie van meetkundige inzichten in de *Elementen* van Euclides, geschreven rond 300 voor Christus. Om toegang te krijgen tot cultuurschatten zoals deze moet je vertrouwd raken met de gebruikte manier van presenteren.

Formele bewijzen leren begrijpen en zelf opzetten vormde eeuwenlang de hoofdmoot van het wiskunde onderwijs. Vandaag de dag is dat niet meer zo, omdat 'inzicht verwerven' belangrijker wordt geacht dan vaardigheid krijgen in het bewijzen. Bewijs en inzicht zijn echter twee kanten van dezelfde medaille: door te proberen bewijzen te leveren of doorgronden kom je tot inzicht, en om inzicht te communiceren zijn bewijzen nodig.

Over de auteurs

Jan van Eijck is filosoof, computationeel taalkundige en toegepast logicus. Hij is als onderzoeker verbonden aan het Centrum voor Wiskunde en Informatica in Amsterdam, en hij is hoogleraar aan de Faculteit Letteren van de Universiteit Utrecht.

Albert Visser is hoogleraar logica en filosofie van wiskunde en kenleer aan de Faculteit Filosofie van de Universiteit Utrecht. Een van zijn interessegebieden is bewijstheorie.

Exact in Context is een reeks die speciaal wordt ontwikkeld voor het voortgezet onderwijs. De reeks biedt informatie over ontwikkelingen in de beta wetenschap die het gezicht van de moderne informatiemaatschappij mede bepalen, met aandacht voor de historische context. De serie is op vele manieren en op vele niveaus te gebruiken.

Website bij dit boek: `http://www.cwi.nl/~jve/qed/`.